

PTU 030008

# **AUTOMATIC LOG-IN SYSTEM, AUTOMATIC LOG-IN METHOD, AUTOMATIC LOG-IN PROGRAM, AND STORAGE MEDIUM**

**Publication number:** JP2004151863 (A)

**Publication date:** 2004-05-27

**Inventor(s):** KATO TAKATOSHI; WAKASA SHIGEKI; NAKAYAMA HIROSHI; NAGASHIMA  
ATSUSHI +

**Applicant(s):** SONY CORP +

**Classification:**

**- International:** G06F13/00; G06F15/00; G06F21/20; G09C1/00; H04L9/32; G06F13/00; G06F15/00;  
G06F21/20; G09C1/00; H04L9/32; (IPC1-7): G06F13/00; G06F15/00; G09C1/00;  
H04L9/32

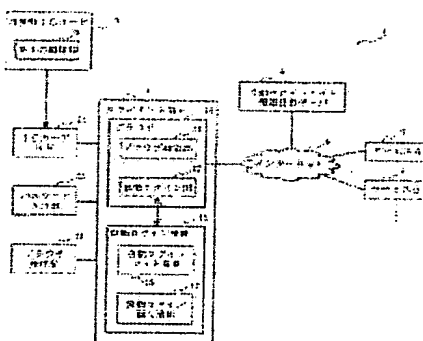
**- European:**

**Application number:** JP20020314680 20021029

**Priority number(s):** JP20020314680 20021029

## **Abstract of JP 2004151863 (A)**

**PROBLEM TO BE SOLVED:** To provide an automatic log-in system having high safety in terms of security, and reducing the load of any log-in operation to each site. ; **SOLUTION:** A browser 10 is provided with a browser functioning part 11 for exhibiting a browser function and an automatic log-in part 12 for automatically logging-in a service site. Automatic log-in information 15 is configured of automatic log-in site information 16 which can be decoded with first key information 9 acquired from a non-contact IC card 7 and automatic log-in personal information 17 which can be multiplexed with the first key information 9 and an automatic log-in password. When the browser functioning part 11 performs access to a log-in page registered with the automatic log-in information 15, the automatic log-in part 12 generates a log-in request by using the automatic log-in information 15, and transmits it to a server 5. ; **COPYRIGHT:** (C)2004,JPO



Data supplied from the *espacenet* database — Worldwide

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-151863

(P2004-151863A)

(43) 公開日 平成16年5月27日(2004.5.27)

(51) Int. Cl.<sup>7</sup>

G06F 15/00

G06F 13/00

G09C 1/00

H04L 9/32

F I

G06F 15/00 330B

G06F 15/00 330G

G06F 13/00 510S

G09C 1/00 640E

H04L 9/00 673A

テーマコード(参考)

5B085

5J104

審査請求 未請求 請求項の数 31 O L (全 36 頁) 最終頁に続く

(21) 出願番号 特願2002-314680 (P2002-314680)

(22) 出願日 平成14年10月29日(2002.10.29)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100096655

弁理士 川井 隆

(74) 代理人 100091225

弁理士 仲野 均

(72) 発明者 加藤 孝俊

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

(72) 発明者 若狭 繁基

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

最終頁に続く

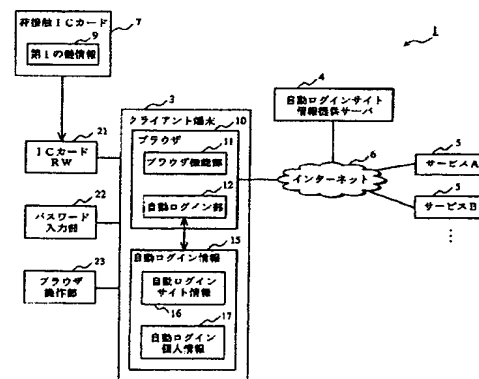
(54) 【発明の名称】 自動ログインシステム、自動ログイン方法、自動ログインプログラム、及び記憶媒体

(57) 【要約】

【課題】セキュリティ面で安全性が高く、各サイトへのログイン操作の負担を軽減することができる自動ログインシステムなどを提供すること。

【解決手段】ブラウザ10は、ブラウザ機能を発揮するブラウザ機能部11と、サービスサイトに自動的にログインする自動ログイン部12を備えている。自動ログイン情報15は、非接触ICカード7から取得した第1の鍵情報9で復号化できる自動ログインサイト情報16と、第1の鍵情報9と自動ログインパスワードで復号化できる自動ログイン個人情報17から構成されている。自動ログイン部12は、ブラウザ機能部11が自動ログイン情報15で登録してあるログインページにアクセスすると、自動ログイン情報15を用いてログインリンクエントを生成し、サーバ5に送信する。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項1】

サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする自動ログイン装置を備えた自動ログインシステムであって、

前記自動ログイン装置は、

鍵情報を記憶したICカードから前記鍵情報を取得する鍵情報取得手段と、

自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化手段と、

前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン手段と、

を具備したことを特徴とする自動ログインシステム。

## 【請求項2】

前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供サーバを備えたことを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項3】

前記ICカードは、非接触型ICカードであることを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項4】

前記自動ログイン装置は、

前記自動ログイン情報記憶手段を具備したことを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項5】

前記ICカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記自動ログイン装置は、前記ICカードから前記自動ログイン情報の少なくとも一部を取得することを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項6】

前記自動ログイン情報は、サービスサイト毎に構成されており、

前記自動ログイン装置は、

ユーザがサービスサイトを選択するサイト選択手段と、

前記選択したサービスサイトに対する前記自動ログイン情報を検索する自動ログイン情報検索手段と、

を具備し、

前記自動ログイン手段は、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインすることを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項7】

前記自動ログイン情報は、

自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、

前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、

から構成されていることを特徴とする請求項1に記載の自動ログインシステム。

## 【請求項8】

前記自動ログイン装置は、第2の鍵情報を取得する第2の鍵情報取得手段を具備し、

前記自動ログイン個人情報は、前記ICカードから取得した鍵情報と、前記取得した第2の鍵情報を用いて復号化可能に暗号化されており、

前記復号化手段は、前記鍵情報と前記第2の鍵情報を用いて前記自動ログイン個人情報復号化することを特徴とする請求項7に記載の自動ログインシステム。

## 【請求項9】

10

20

30

40

50

前記自動ログインサイト情報と、前記自動ログイン個人情報とは、サービスサイト毎に対応付けられて構成されており、

前記自動ログイン装置は、

ユーザがサービスサイトを選択するサイト選択手段と、

前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索手段と、

前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を検索する自動ログイン個人情報検索手段と、

前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを生成するログインリクエスト生成手段と、を具備し、

前記自動ログイン手段は、前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信することを特徴とする請求項7に記載の自動ログインシステム。

#### 【請求項10】

前記自動ログイン装置は、

前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記第1の鍵情報と前記第2の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加手段を具備したことを特徴とする請求項8に記載の自動ログインシステム。

#### 【請求項11】

前記自動ログイン装置が、

前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備したことを特徴とする請求項7に記載の自動ログインシステム。

#### 【請求項12】

前記自動ログイン情報記憶手段は、前記自動ログイン装置に着脱可能な記憶媒体に前記自動ログイン個人情報を記憶することを特徴とする請求項11に記載の自動ログインシステム。

#### 【請求項13】

請求項10に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報提供サーバを備えたことを特徴とする請求項10に記載の自動ログインシステム。

#### 【請求項14】

前記自動ログイン装置は、

前記ICカードが前記自動ログイン装置にセットされているか否かを検出する検出手段と、

前記検出手段で前記ICカードがセットされていないと検出した場合に、前記自動ログイン装置に対する入力をロックするロック機構と、

を具備したことを特徴とする請求項1に記載の自動ログインシステム。

#### 【請求項15】

請求項12に記載の記憶媒体であって、自動ログイン個人情報を記憶し、前記クライアント端末に着脱可能な記憶媒体。

#### 【請求項16】

サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする自動ログイン装置を用いた自動ログイン方法であって、

前記自動ログイン装置は、鍵情報取得手段と、復号化手段と、自動ログイン手段と、を備え、

10

20

30

40

50

前記鍵情報取得手段で、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得ステップと、

自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて前記復号化手段で復号化する復号化ステップと、

前記復号化した自動ログイン情報を用いて、前記自動ログイン手段で、前記サービスサイトに自動ログインする自動ログインステップと、

から構成されたことを特徴とする自動ログイン方法。

【請求項１７】

自動ログイン情報提供サーバが、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。

10

【請求項１８】

前記ＩＣカードは、非接触型ＩＣカードであることを特徴とする請求項１６に記載の自動ログイン方法。

【請求項１９】

前記自動ログイン装置は、前記自動ログイン情報記憶手段を具備し、

前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。

【請求項２０】

前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記ＩＣカードから前記自動ログイン情報の少なくとも一部を取得する取得ステップを備えたことを特徴とする請求項１６に記載の自動ログイン方法。

20

【請求項２１】

前記自動ログイン情報は、サービスサイト毎に構成されており、

前記自動ログイン装置は、サイト選択手段と、自動ログイン情報検索手段と、を備え、

前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、

前記選択したサービスサイトに対する前記自動ログイン情報を、前記自動ログイン情報検索手段で検索する自動ログイン情報検索ステップと、

を備え、

30

前記自動ログインステップでは、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインすることを特徴とする請求項１６に記載の自動ログイン方法。

【請求項２２】

前記自動ログイン情報は、

自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、

前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、

から構成されていることを特徴とする請求項１６に記載の自動ログイン方法。

40

【請求項２３】

前記自動ログイン装置は、第２の鍵情報取得手段を具備し、

前記第２の鍵情報取得手段で、第２の鍵情報を取得する第２の鍵情報取得ステップを備え、

、

前記復号化ステップで、前記自動ログイン個人情報と、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化することを特徴とする請求項２２に記載の自動ログイン方法。

【請求項２４】

前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、

50

前記自動ログイン装置は、サイト選択手段と、自動ログインサイト情報検索手段と、自動ログイン個人情報検索手段と、ログインリクエスト生成手段と、を具備し、  
前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、  
前記自動ログインサイト情報検索手段で、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索ステップと、  
前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を、前記自動ログイン個人情報検索手段で検索する自動ログイン個人情報検索ステップと、  
前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを前記ログインリクエスト生成手段で生成するログインリクエスト生成ステップと、  
前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信する送信ステップと、  
を備えたことを特徴とする請求項 22 に記載の自動ログイン方法。

【請求項 25】

前記自動ログイン装置は、自動ログイン個人情報追加手段を具備し、  
前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記自動ログイン個人情報追加手段で、前記第 1 の鍵情報と前記第 2 の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加ステップを具備したことを特徴とする請求項 23 に記載の自動ログイン方法。

【請求項 26】

前記自動ログイン装置が、  
前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備し、  
前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えたことを特徴とする請求項 22 に記載の自動ログイン方法。

【請求項 27】

前記自動ログイン情報取得ステップでは、前記自動ログイン装置に着脱可能な記憶媒体から前記自動ログイン個人情報を取得することを特徴とする請求項 26 に記載の自動ログイン方法。

【請求項 28】

自動ログインサイト情報提供サーバから、請求項 25 に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報送信ステップを備えたことを特徴とする請求項 25 に記載の自動ログイン方法。

【請求項 29】

前記自動ログイン装置は、検出手段と、ロック機構とを具備し、  
前記検出手段で、前記 IC カードが前記自動ログイン装置にセットされているか否かを検出する検出ステップと、  
前記検出手段で前記 IC カードがセットされていないと検出した場合に、前記ロック機構で、前記自動ログイン装置に対する入力をロックするロックステップと、  
を備えたことを特徴とする請求項 16 に記載の自動ログイン方法。

【請求項 30】

サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムであって、  
鍵情報を記憶した IC カードから前記鍵情報を取得する鍵情報取得機能と、  
自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、  
前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、

10

20

30

40

50

をコンピュータで実現するための自動ログインプログラム。

【請求項 31】

サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、

鍵情報を記憶したICカードから前記鍵情報を取得する鍵情報取得機能と、

自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、

前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、

をコンピュータで実現するための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、自動ログインシステムなどに関し、特に、ICカードに記憶されている鍵情報を用いて、ログインに必要な情報を復号化し、これを用いてサービスサイトに自動ログインするものに関する。

【0002】

【従来の技術】

近年の急速なインターネットの普及により、誰でもインターネットを介して様々なサービスを享受することができるようになってきた。

また、インターネット上で提供されるサービスも、ニュース、天気予報、テレビ番組表、広告など、ユーザに情報を提供するものの他、銀行預金の管理、有価証券の売買などユーザの資産を管理するものまで多岐に渡っている。

これら、インターネット上でサービスを提供するサービスサイトには、ユーザが入力したログインIDやパスワードなどからユーザを認証するものがある。

このようなサービスサイトにアクセスする際、ユーザは、当該サービスサイトに設定してあるログインIDやパスワードをキーボードなどの入力装置を用いて入力する。

このようにして、ユーザを認証することにより、ユーザに固有のサービスを提供したり、システムのセキュリティを高めたりしている。

【0003】

図17は、従来のログイン方法を説明するための図である。

クライアント端末1001は、インターネット1002を介してサービスAを提供するサーバ1005とサービスBを提供するサーバ1006に接続可能に配設されている。ここで、サービスサイトA、Bにログインするために、ログインIDとパスワードを入力するものとする。

この場合、クライアント端末1001からサーバ1002にアクセスしてサーバ1002が提供するサービスAを利用するためには、サービスAを提供するログインページ（例えば、「`http://www.serverA.com/serviceA/login.html`」などのURLで特定される）にアクセスし、ログインIDとパスワードをキーボードから入力する。

【0004】

また、クライアント端末1001から、サーバBが提供するサービスBを利用するためには、サービスBのログインページ（例えば、「`http://www.serverB.com/serviceB/login.html`」などのURLで特定される）にアクセスし、ログインIDとパスワードを入力する。

なお、通常はログインに使用するログインIDとパスワードは、サイト毎に異なっており、インターネット上の各サイトにログインする場合、ユーザは、キーボードなどを用いて

10

20

30

40

50

、その都度、当該サイト用のログインIDとパスワードを入力する必要がある。  
このような、キーボードからのログインID及びパスワードの入力の煩わしさを改善し、  
キーボードよりログインIDとパスワードの入力を行わずに目的のサイトにログインする  
技術として次のものがある。

【0005】

【特許文献1】特開2002-175281号公報

【特許文献2】特開2002-41380号公報

【0006】

上記特許文献1の「ネットワークログインシステム」は、パーソナルコンピュータとIC  
カード内蔵の携帯端末から暗証番号を入力して、ネットワーク上のサイトへの自動ログイン  
を行う技術である。ICカードにはネットワーク接続権限の有無や、ログイン時の暗証  
番号が記録されており、入力された暗証番号の認証を経て、ネットワークへの接続が許可  
される。

また、上記特許文献2の「データ処理システム及び方法」は、クライアント端末側でサー  
バ側が提供するインターネットサービスへのログインリクエストをブックマークとして管  
理しておき、これを用いて認証処理を省いて自動ログインを行うものである。より詳細に  
は、このブックマークには、認証を受けるサイトへのログインID、及びパスワードを暗  
号化した情報を含むサイトURLが登録されており、当該ブックマークから登録されたU  
RLを選択することで、認証サイトはログイン情報を抽出して認証を行う。

【0007】

【発明が解決しようとする課題】

ところが、上記特許文献1の技術は、ある特定のシステムへのログイン方法を提供してい  
り、インターネット上の複数サイトのサーバへの（個々のサービスでログインIDとパス  
ワードが異なる）ログインを自動で行う汎用的な仕組みではないという問題があった。ま  
た、ICカード内認証を経て、認証結果のみがネットワークへ送信されるものであり、認  
証を必要とする複数サイトへの自動ログインするものではない。

また、上記特許文献2の技術は、クライアント端末が第三者の手に渡った場合に、セキ  
ュリティの面から問題があった。即ち、ブックマークを登録しているクライアント端末を自  
由に他人が使える環境にある場合、誰もが自動ログインできてしまう。

【0008】

そこで、本発明の目的は、セキュリティ面で安全性が高く、各サイトへのログイン操作の  
負担を軽減することができる自動ログインシステムなどを提供することである。

【0009】

【課題を解決するための手段】

本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が  
必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にロ  
グインする自動ログイン装置を備えた自動ログインシステムであって、前記自動ログイン  
装置は、鍵情報を記憶したICカードから前記鍵情報を取得する鍵情報取得手段と、自動  
ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した  
鍵情報を用いて復号化する復号化手段と、前記復号化した自動ログイン情報を用いて前記  
サービスサイトに自動ログインする自動ログイン手段と、を具備したことを特徴とする自  
動ログインシステムを提供する（第1の構成）。

第1の構成で、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供す  
る自動ログイン情報提供サーバを備えるように構成することができる（第2の構成）。

また、第1の構成において、前記ICカードは、非接触型ICカードであるように構成す  
ることができる（第3の構成）。

また、第1の構成において、前記自動ログイン装置は、前記自動ログイン情報記憶手段を  
具備するように構成することができる（第4の構成）。

また、第1の構成において、前記ICカードは、前記自動ログイン情報の少なくとも一部  
を記憶しており、前記自動ログイン装置は、前記ICカードから前記自動ログイン情報の

10

20

30

40

50



少なくとも一部を取得するように構成することができ(第5の構成)。

更に、第1の構成において、前記自動ログイン情報は、サービスサイト毎に構成されており、前記自動ログイン装置は、ユーザがサービスサイトを選択するサイト選択手段と、前記選択したサービスサイトに対する前記自動ログイン情報を検索する自動ログイン情報検索手段と、を具備し、前記自動ログイン手段は、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインするように構成することができ(第6の構成)。

また、第1の構成において、前記自動ログイン情報は、自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリンクエント情報と、を有する自動ログインサイト情報と、前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、から構成されているように構成することができ(第7の構成)。

また、第7の構成において、前記自動ログイン装置は、第2の鍵情報を取得する第2の鍵情報取得手段を具備し、前記自動ログイン個人情報は、前記ICカードから取得した鍵情報と、前記取得した第2の鍵情報を用いて復号化可能に暗号化されており、前記復号化手段は、前記鍵情報と前記第2の鍵情報を用いて前記自動ログイン個人情報復号化するように構成することができ(第8の構成)。

また、第7の構成において、前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、前記自動ログイン装置は、ユーザがサービスサイトを選択するサイト選択手段と、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索手段と、前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報を検索する自動ログイン個人情報検索手段と、前記検索した自動ログインサイト情報に含まれるログインリンクエント情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリンクエントを生成するログインリンクエント生成手段と、を具備し、前記自動ログイン手段は、前記生成したログインリンクエントを前記選択したサービスサイトが設けられたサービス提供サーバに送信するように構成することができ(第9の構成)。

第8の構成において、前記自動ログイン装置は、前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記第1の鍵情報と前記第2の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加手段を具備するように構成することができ(第10の構成)。

第7の構成において、前記自動ログイン装置が、前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備するように構成することができ(第11の構成)。

第11の構成において、前記自動ログイン情報記憶手段は、前記自動ログイン装置に着脱可能な記憶媒体に前記自動ログイン個人情報を記憶するように構成することができ(第12の構成)。

第10の構成において、請求項10に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報提供サーバを備えるように構成することができ(第13の構成)。

第1の構成において、前記自動ログイン装置は、前記ICカードが前記自動ログイン装置にセットされているか否かを検出する検出手段と、前記検出手段で前記ICカードがセットされていないと検出した場合に、前記自動ログイン装置に対する入力をロックするロック機構と、を具備するように構成することができ(第14の構成)。

また、本発明は、前記目的を達成するために、第12の構成に記載の記憶媒体であって、自動ログイン個人情報を記憶し、前記クライアント端末に着脱可能な記憶媒体を提供する。

また、本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動

10

20

30

40

50

的にログインする自動ログイン装置を用いた自動ログイン方法であって、前記自動ログイン装置は、鍵情報取得手段と、復号化手段と、自動ログイン手段と、を備え、前記鍵情報取得手段で、鍵情報を記憶したＩＣカードから前記鍵情報を取得する鍵情報取得ステップと、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて前記復号化手段で復号化する復号化ステップと、前記復号化した自動ログイン情報を用いて、前記自動ログイン手段で、前記サービスサイトに自動ログインする自動ログインステップと、から構成されたことを特徴とする自動ログイン方法を提供する（第１の方法）。

第１の方法において、自動ログイン情報提供サーバが、前記自動ログイン情報の少なくとも一部を前記自動ログイン装置に提供する自動ログイン情報提供ステップを備えるように構成することができる（第２の方法）。

第１の方法において、前記ＩＣカードは、非接触型ＩＣカードであるように構成することができる（第３の方法）。

第１の方法において、前記自動ログイン装置は、前記自動ログイン情報記憶手段を具備し、前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えるように構成することができる（第４の方法）。

第１の方法において、前記ＩＣカードは、前記自動ログイン情報の少なくとも一部を記憶しており、前記ＩＣカードから前記自動ログイン情報の少なくとも一部を取得する取得ステップを備えるように構成することができる（第５の方法）。

第１の方法において、前記自動ログイン情報は、サービスサイト毎に構成されており、前記自動ログイン装置は、サイト選択手段と、自動ログイン情報検索手段と、を備え、前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、前記選択したサービスサイトに対する前記自動ログイン情報を、前記自動ログイン情報検索手段で検索する自動ログイン情報検索ステップと、を備え、前記自動ログインステップでは、前記検索した自動ログイン情報を用いて前記サービスサイトに自動ログインするように構成することができる（第６の方法）。

第１の方法において、前記自動ログイン情報は、自動ログイン対象のサービスサイトを特定するサービスサイト特定情報と、前記サービスサイト特定情報で特定される前記サービスサイトへのログイン処理を前記サービス提供サーバに要求するログインリクエスト情報と、を有する自動ログインサイト情報と、前記サービス提供サーバがユーザを認証するのに要するユーザ認証情報を有する自動ログイン個人情報と、から構成されているように構成することができる（第７の構成）。

第７の構成において、前記自動ログイン装置は、第２の鍵情報取得手段を具備し、前記第２の鍵情報取得手段で、第２の鍵情報を取得する第２の鍵情報取得ステップを備え、前記復号化ステップで、前記自動ログイン個人情報を、前記ＩＣカードから取得した鍵情報と、前記取得した第２の鍵情報を用いて復号化するよう構成することができる（第８の構成）。

第７の構成において、前記自動ログインサイト情報と、前記自動ログイン個人情報は、サービスサイト毎に対応付けられて構成されており、前記自動ログイン装置は、サイト選択手段と、自動ログインサイト情報検索手段と、自動ログイン個人情報検索手段と、ログインリクエスト生成手段と、を具備し、前記サイト選択手段で、ユーザがサービスサイトを選択するサイト選択ステップと、前記自動ログインサイト情報検索手段で、前記選択したサービスサイトに対する前記自動ログインサイト情報を検索する自動ログインサイト情報検索ステップと、前記検索した自動ログインサイト情報に対応付けられた自動ログイン個人情報と、前記自動ログイン個人情報検索手段で検索する自動ログイン個人情報検索ステップと、前記検索した自動ログインサイト情報に含まれるログインリクエスト情報と前記検索した自動ログイン個人情報に含まれるユーザ認証情報とを用いてサービス提供サーバがログイン処理を行うのに用いるログインリクエストを前記ログインリクエスト生成手段で生成するログインリクエスト生成ステップと、前記生成したログインリクエストを前記選択したサービスサイトが設けられたサービス提供サーバに送信する送信ステップと、

10

20

30

40

50

を備えたるように構成することができる（第 9 の方法）。

第 8 の方法において、前記自動ログイン装置は、自動ログイン個人情報追加手段を具備し、前記検索された前記自動ログインサイト情報に対応する前記自動ログイン個人情報が検索できなかった場合、ユーザから入力される情報を用いて前記自動ログインサイト情報に対応する自動ログイン個人情報を、前記自動ログイン個人情報追加手段で、前記第 1 の鍵情報と前記第 2 の鍵情報で復号化可能に暗号化して追加する自動ログイン個人情報追加ステップを具備するように構成することができる（第 10 の方法）。

第 7 の方法において、前記自動ログイン装置が、前記自動ログイン情報を記憶する自動ログイン情報記憶手段を具備し、前記自動ログイン情報記憶手段から、前記自動ログイン情報を取得する自動ログイン情報取得ステップを備えるように構成することができる（第 11 の方法）。

10

第 11 の方法において、前記自動ログイン情報取得ステップでは、前記自動ログイン装置に着脱可能な記憶媒体から前記自動ログイン個人情報を取得するように構成することができる（第 12 の方法）。

第 10 の方法において、自動ログインサイト情報提供サーバから、請求項 25 に記載の自動ログインサイト情報を前記自動ログイン装置に送信する自動ログインサイト情報送信ステップを備えるように構成することができる（第 13 の方法）。

第 1 の方法において、前記自動ログイン装置は、検出手段と、ロック機構とを具備し、前記検出手段で、前記 IC カードが前記自動ログイン装置にセットされているか否かを検出する検出ステップと、前記検出手段で前記 IC カードがセットされていないと検出した場合に、前記ロック機構で、前記自動ログイン装置に対する入力をロックするロックステップと、を備えるように構成することができる（第 14 の方法）。

20

また、本発明は、前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムであって、鍵情報を記憶した IC カードから前記鍵情報を取得する鍵情報取得機能と、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、をコンピュータで実現するための自動ログインプログラムを提供する。

30

更に、本発明は前記目的を達成するために、サービス提供サーバに設けられたログイン処理が必要なサービスサイトにログインする際に使用する自動ログイン情報を用いて自動的にログインする機能をコンピュータに発揮させるための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体であって、鍵情報を記憶した IC カードから前記鍵情報を取得する鍵情報取得機能と、自動ログイン情報記憶手段に記憶され、暗号化された前記自動ログイン情報を、前記取得した鍵情報を用いて復号化する復号化機能と、前記復号化した自動ログイン情報を用いて前記サービスサイトに自動ログインする自動ログイン機能と、をコンピュータで実現するための自動ログインプログラムを記憶したコンピュータが読み取り可能な記憶媒体を提供する。

【0010】

【発明の実施の形態】

（第 1 の実施の形態）

以下、本発明の好適な第 1 の実施の形態について詳細に説明する。

（1）実施形態の概要

本実施の形態は、インターネットを介して提供される各サービスサイトへのログイン認証を IC カードのような記録媒体に記憶した鍵情報を用いるなどして自動的に行うものである。この鍵情報はログインする際に必要なログイン情報を復号化するのに用いられる。ログイン情報を用いてログインすることにより、従来キーボードから入力していたログイン ID とパスワードを入力する手間を省き、ユーザの負担を軽減することができる。また、

各サービスサイトへのログインには、IC カードが必要となり、セキュリティ面でも安

50

全性を確保している。

本実施の形態の手法は、インターネット上のあらゆるサービスサイトへのログインで利用することができる。

#### 【0011】

クライアント端末 8 (図 1) は、インターネット 6 を介してサービス A、B、 を提供するサーバ 5、サーバ 5、 (以下サーバ 5) に接続可能に配設されている。サーバ 5 は、ユーザがログインを行うことにより、各種サービスを提供する。

クライアント端末 8 に搭載されたブラウザ 10 は、自動ログイン部 12 を備えており、自動ログイン情報 15 を用いてサーバ 5 に自動的にログインする機能を備えている。

自動ログイン情報 15 は、自動ログインサイト情報 16 と、自動ログイン個人情報 17 から構成されている。自動ログインサイト情報 16、自動ログイン個人情報 17 は、何れも暗号化されており、自動ログインサイト情報 16 は、ユーザが有する非接触 IC カード 7 に記憶されている第 1 の鍵情報 9 で復号化され、自動ログイン個人情報 17 は、第 1 の鍵情報 9 と、ユーザが入力する自動ログイン用パスワード (第 2 の鍵情報) で復号化される。

10

#### 【0012】

自動ログインサイト情報 16 (図 2) は、サーバ 5 が提供するサービスを識別するサービス名称 141、ログインページ (ログイン ID やパスワードなどの認証情報をユーザが入力するためのログイン認証ページ) の URL であるログインページ情報 142、ログインする際にサーバ 5 に送信する情報であるログインリクエスト情報 143 から構成されてい

20

る。一方、自動ログイン個人情報 17 は、サーバ 5 が提供するサービスを識別するサービス名称 145、ログインリクエスト情報 143 に付属させるパラメータ値 (引数) 146、147、148、 から構成される。各パラメータ値は、ユーザがサーバ 5 にログインする際に必要となるログイン ID やパスワードなどのサーバ 5 がユーザを認証するための情報である。

自動ログインサイト情報 16 と、自動ログイン個人情報 17 は、サービス名称 141 とサービス名称 145 により互いも付けられており、一対一の対応関係がとられている。

#### 【0013】

自動ログイン部 12 は、ブラウザ 10 に入力された URL を監視しており、入力された URL がログインページに登録されている URL に一致すると、その該当するサービス名称 141 のログインリクエスト情報 143 のパラメータに、自動ログイン個人情報 17 のパラメータ値 146、147、 を代入してログインリクエストを生成し、サーバ 5 に送信する。

30

サーバ 5 は、クライアント端末 8 からログインリクエストを受け取り、これを用いてユーザを認証し、ログイン処理 (ログイン認証処理) を行う。

#### 【0014】

このように、ブラウザ 10 に入力される URL を監視して、その結果、接続先のサービスサイトが自動ログイン情報 15 に登録してあるものである場合、自動的にログインを行うことができる。そのため、ブラウザ 10 は、ログイン手続きでユーザが行う負担を軽減することができる。

40

更に、今後、インターネットブラウザ機能を持ったテレビなどの情報家電の普及が予想される。このような情報家電は通常キーボードなどの入力デバイスを持たない場合が多いと考えられ、その場合、リモコンを用いてログイン ID とパスワードを入力すると思われる。この場合、ログイン ID とパスワードの入力がユーザにとって負担になると共に、ログイン ID やパスワードが第三者の手に渡った場合、どのクライアント端末からでもログイン ID とパスワードを入力することが可能であり、セキュリティ的にも問題がある。

これら情報家電に、本実施の形態のブラウザ 10 を搭載すると、ユーザは、非接触 IC カード 7 と自動ログイン用パスワードを用いて自動的にログインすることになり、これらのパラメータの入力が容易になると共に、セキュリティを高めることができる。

50

## 【0015】

## (2) 実施形態の詳細

図1は、本実施の形態のシステム構成を説明するための図である。

自動ログインシステム1は、非接触ICカード7、クライアント端末8、インターネット6、自動ログインサイト情報提供サーバ4、サーバ5、5、（以下サーバ5）から構成されている。

非接触ICカード7は、非接触でデータの送受信を行うデータ送受信手段、受信したデータを記憶する記憶手段などを備えており、クライアント端末8に設けられたICカードRW（リーダライタ）21を介して、クライアント端末8とデータの送受信を行うことができる。また、演算手段を備えることも可能である。

非接触ICカード7は、ループ状のアンテナと半導体チップを内蔵しており、ICカードRW21に近づけると、ICカードRW21が発する電磁波をこのアンテナで受信して起電力を得ると共に、データの送受信を行う。

## 【0016】

本実施の形態では、非接触ICカード7に第1の鍵情報9を記憶しておき、これをICカードRW21で読み取る。

第1の鍵情報9は、暗号鍵などの鍵情報を非接触ICカード7に記憶させてもよいし、あるいは、非接触ICカード7に予めICカードRW21で読み取り可能に割り当てられている固有IDを用いてもよい。固有IDは、非接触ICカード7毎に一意的に割り当ててあり、固有IDにより、非接触ICカード7を特定することができる。本実施の形態では、固有IDを第1の鍵情報9として用いるものとする。このように、ICカードRW21は鍵情報取得手段を構成している。

## 【0017】

クライアント端末8は、ブラウザ10、自動ログイン情報15、ICカードRW21、パスワード入力部22、ブラウザ操作部23を備えており、インターネット6を介して、自動ログインサイト情報提供サーバ4（自動ログイン情報提供サーバ）、サーバ5に接続可能に配設されている。

詳細は後述するが、クライアント端末8は、例えば、パーソナルコンピュータを用いて構成されている。

ブラウザ10は起動するとICカードRW21を監視し、非接触ICカード7がICカードRW21に接近すると、非接触ICカード7から第1の鍵情報9を読み取り、ブラウザ10に渡す。ブラウザ10は、一定時間毎に非接触ICカード7の有無を監視している。パスワード入力部22は、例えば、ディスプレイに表示された自動ログインパスワード入力ダイアログと、キーボードなどから構成され、ユーザがキーボードなどから入力した自動ログインパスワードを取得する。パスワード入力部22で取得した自動ログインパスワードは、後述する第2の鍵情報として使用される。

このように、パスワード入力部22は、第2の鍵情報取得手段を構成している。

## 【0018】

ブラウザ操作部23は、ブラウザ10が備えた各機能を実行するためのユーザインターフェースであり、例えば、ディスプレイに表示されたブラウザ画面、情報を入力するためのキーボード、マウスなどから構成される。

ユーザは、ブラウザ画面を見ながら、キーボード、マウスなどから情報を入力し、ブラウザ10が備えた各機能を実行することができる。

ブラウザ操作部23からのURLの入力は、例えば、サービスサイトを表したアイコンをクリックしたり、あるいはブラウザ画面上に設けられたURL欄にキーボードからURLを入力するなどして行うことができる。

また、ユーザがホームページでログインページにジャンプするボタンをクリックした場合、サーバ5からログインページが送信されてきて、URL欄にこのログインページのURLが入力される。

## 【0019】

10

20

30

40

ブラウザ 10 は、ブラウザ機能部 11 と自動ログイン部 12 から構成されている。ブラウザ機能部 11 は、通常のブラウズを行う機能部であり、インターネット 6 上に開設されたサービスサイトにアクセスして、これらサービスサイトが提供するサービスを利用するのに用いる。

ブラウザ機能部 11 は、例えば、入力された URL で指定されるサービスサイトにアクセスし、これに対してサービスサイトが送信してくるホームページを表示する。

また、ユーザがこれらホームページ上で入力した情報を所定のサーバ 5 に送信する。

ユーザは、ブラウザ機能部 11 を用いてサービスサイトが提供するサービスを利用することにより、例えば、必要な情報を検索したり、オンラインショッピングを行ったり、あるいは、預金口座や株式売買を管理したり、更には、ゲームや動画を見たりなど、様々なコンテンツを利用することができる。

10

#### 【0020】

自動ログイン部 12 は、ユーザがログイン認証を要するサービスサイトにアクセスした際に、ログイン認証手続きを自動的に代行する機能部である。

詳細は後述するが、自動ログイン部 12 は、ブラウザ機能部 11 がアクセスする URL を監視しており、後述の自動ログインサイト情報 16 に登録してある URL (ログインページの URL) にアクセスした場合に、ユーザに代わってログインリクエストを作成してサーバ 5 に送信する。

ログインリクエストとは、サーバ 5 側で、ログイン処理を行う認証処理プログラム (例えば CGI (Common Gateway Interface) プログラムにより構成される) を動作させ、ユーザを認証させるための情報である。通常は、ユーザがログイン画面で入力したログイン ID、パスワードなどをパラメータ値としてサーバ 5 に送信する。サーバ 5 では、このログインリクエストによりログイン認証プログラムを動作させ、ログインリクエストに付属するパラメータ値 (ログイン ID、パスワードなど) を用いてユーザをログイン認証する。

20

#### 【0021】

自動ログイン情報 15 は、自動ログイン部 12 が URL を監視したり、ログインリクエストを自動生成するのに用いる情報から構成されている。

後に詳細に説明するが、自動ログインサイト情報 16 は、ログインページやログインリクエストを生成するためのログインリクエスト情報など、公になっている情報から構成されている。

30

自動ログインサイト情報 16 は、非接触 IC カード 7 から取り込んだ第 1 の鍵情報 9 で復号化可能に暗号化されている。自動ログインサイト情報 16 は、後述する自動ログインサイト情報提供サーバ 4 からインターネット 6 を経由してダウンロードしたものである。また、自動ログインサイト情報提供サーバ 4 から更新情報を受信し、これを用いてクライアント端末 3 は自動ログインサイト情報 16 を最新のものに更新することができる。

自動ログイン個人情報 17 は、ログイン ID やパスワードなど、ユーザに固有なユーザ認証用の情報 (ユーザ認証情報) などから構成されている。

自動ログイン個人情報 17 は、第 1 の鍵情報 9、及びパスワード入力部 22 から取得した自動ログインパスワードの双方を用いて復号化できるように暗号化されている。この場合、自動ログインパスワードは、第 2 の鍵情報を構成している。

40

#### 【0022】

自動ログインサイト情報提供サーバ 4 は、クライアント端末 3 に自動ログインサイト情報 16 や、自動ログインサイト情報 16 を更新するための更新情報を提供するためのサーバ装置である。

自動ログインサイト情報提供サーバ 4 では、自動ログインサイト情報提供サーバ 4 の事業者が、クライアント端末 3 で自動ログインサイト情報 16 に新たなサービスサイトを追加したり、あるいは削除したりするための更新情報を管理している。

この更新情報は、クライアント端末 3 で、自動ログインサイト情報 16 を全て上書きするように構成することもできるし、あるいは、最新の自動ログインサイト情報と、クライ

50

ント端末 3 の自動ログインサイト情報 1 6 の差分を送るように構成することもできる。

【0023】

サーバ 5、5、 は、サービス A、サービス B、 など、各種のサービスを提供するサービスサイトが開設された WWW (World Wide Web) サーバである。図 1 は、それぞれのサーバ 5 に 1 つずつサービスサイトが開設されているが、サービスサイトは URL により一意的に識別できるため、1 つのサーバ 5 に複数のサービスサイトを開設してもよい。

本実施の形態のサービス A、サービス B、 を提供するサービスサイトは、ユーザからログイン ID やパスワードなどの個人認証用の情報を受け取ってログイン認証を行うものとする。

10

【0024】

サービスサイトで提供されるサービスは、例えば、銀行口座の管理、有価証券の売買、電子メールの送受信、オンラインショッピング、会員それぞれ用にカスタマイズされたテレビ番組表、会員制の娯楽サイト、 など各種のものが考えられる。本実施の形態では、何れのサービスサイトもログイン認証を必要とするものである。また、サービスサイトには、有料のものや無料のものがある。

なお、本実施の形態では、自動ログインに関する処理はクライアント端末 3 が行うため、サーバ 5 に自動ログイン用の仕組みを設けるなど、サーバ側の変更は必要ない。

【0025】

本実施の形態では、ネットワークとしてインターネット 6 を考えたが、これに限定するものではなく、例えば、LAN (Local Area Network)、WAN (Wide Area Network)、人工衛星を介したネットワークなど、他の形態のネットワークでもよい。

20

なお、サーバ 5 を WWW サーバとしたが、これに限定するものではなく、ユーザから個人認証用の情報を受信してログイン認証する送受信装置であればよい。

また、本実施の形態では、非接触 IC カード 7 を用いたが、接触式の IC カード、ID カードなど、クライアント端末 3 が第 1 の鍵情報 9 を読み出せる他の記憶媒体を用いてもよい。

更に、第 2 の鍵情報を得るために、パスワード入力部 2 2 から自動ログインパスワードを取得したが、第 2 の鍵情報の取得方法は、これに限定するものではなく、例えば、ユーザの指紋、声紋、目の虹彩など、ユーザを確認できるものであればよい。

30

【0026】

図 2 は、自動ログイン情報 1 5 の論理的な構成の一例をテーブルとして示した図である。このうち、図 2 (a) は、自動ログインサイト情報 1 6 を示し、図 2 (b) は、自動ログイン個人情報 1 7 を示している。

図 2 (a) に示したように、自動ログインサイト情報 1 6 は、サービス名称 1 4 1、ログインページ情報 1 4 2、ログインリクエスト情報 1 4 3 から構成されており、サービス名称 1 4 1 毎に区分されている。

自動ログインサイト情報 1 6 は、第 1 の鍵情報 9 により復号化可能に暗号化されている。サービス名称 1 4 1 は、自動ログインサイト情報 1 6 と自動ログイン個人情報 1 7 とをひも付けして対応させるための情報であり、ここでは、サービスサイトに一意的に割り当てられたサービス名称を用いている。

40

【0027】

ログインページ情報 1 4 2 は、自動ログイン処理の対象となるサービスサイトのログインページの URL である。ログインページ情報 1 4 2 は、自動ログイン部 1 2 (図 1) が、ブラウザ機能部 1 1 で入力された URL を監視するために用いる。

即ち、自動ログイン部 1 2 は、ブラウザ機能部 1 1 で URL が入力されると、この URL とログインページ情報 1 4 2 を比較し、一致するものがある場合に、自動ログイン処理を行う。

【0028】

50

ログインページ情報 142 に登録されている URL は、例えば、「`http://serverA.com/login.html`」といったように構成されており、この場合、サーバ「`serverA`」にある HTML (HyperText Markup Language) ファイル「`login.html`」を特定している。

なお、HTML ファイル「`login.html`」は、ブラウザ機能部 11 にログインページ画面を表示させるための画面データである。

#### 【0029】

ログインリクエスト情報 143 は、サーバ 5 がログイン認証を行うのに用いるログインリクエストを生成するための情報である。

ログインリクエストは、サーバ 5 でログイン処理を要求するための情報であり、一般にパラメータ値 (引数) としてログイン ID やパスワードなどを伴う。

ログインリクエスト情報 143 は、例えば、「`http://serverA.com/login.cgi?lid=%1pwd=%2`」といったような形をしている。

これは、サーバ「`serverA`」のログイン認証プログラム「`login.cgi`」に、パラメータ「`%1`」に付随するパラメータ値 (ログイン ID) と、パラメータ「`%2`」に付随するパラメータ値 (パスワード) を引数として渡すことを意味している。

本実施の形態では、「`%1`」や「`%2`」などのパラメータに付随させるログイン ID やパスワードなどのパラメータ値は、次に説明する自動ログイン個人情報 17 で管理している。

#### 【0030】

図 2 (b) に示したように、自動ログイン個人情報 17 には、サービス名称 145 や、パラメータ値 146、147、その他のパラメータ値 148 などの、ユーザを認証する際に使用するユーザに固有な情報などが含まれている。

自動ログイン個人情報 17 は、サービス名称 145 毎に区分されており、第 1 の鍵情報 9、及び第 2 の鍵情報 (自動ログインパスワード) で復号化可能に暗号化されている。このように、自動ログイン個人情報 17 には、ユーザに固有な情報が含まれているため、第 1 の鍵情報 9 と第 2 の鍵情報を用いないと復号化できないようになっており、セキュリティが高められている。

このため、第三者が非接触 IC カード 7 を取得して第 1 の鍵情報 9 を利用しても、自動ログインパスワードがわからなければ、自動ログイン個人情報 17 を復号化することはできない。

#### 【0031】

サービス名称 145 は、自動ログインサイト情報 16 とひも付けするための情報であり、サービスサイトに一意的に与えられたサービス名称である。

自動ログイン部 12 は、サービス名称 141 と同じサービス名称 145 を検索することにより、自動ログインサイト情報 16 と自動ログイン個人情報 17 をひも付けすることができる。

#### 【0032】

パラメータ値 146 は、ひも付けされたログインリクエスト情報 143 のパラメータ「`%1`」に付随させるためのパラメータ値であり、通常はログイン ID が用いられる。

パラメータ 147 は、ひも付けされたログインリクエスト情報 143 のパラメータ「`%2`」に付随させるためのパラメータ値であり、通常はパスワードが用いられる。

なお、「`%1`」などのパラメータ値を対応させるかは、サーバ 5 で設定できるため、サーバ 5 によっては、「`%1`」にパスワードなど他のパラメータ値が設定されている場合もある。

その他のパラメータ値 148 は、ログインリクエスト情報 143 が更に多くのパラメータ値を必要とする場合に、そのパラメータ値が設定される。このような場合として、例えば、1 回のログイン処理に複数のパスワードを使用する場合などがある。

#### 【0033】

図 3 は、ブラウザ 10 の機能的な構成を説明するための模式図である。

10

20

30

40

50



図 3 に示したように、ブラウザ 10 は、ブラウザ機能部 11、暗号・復号部 31、自動追加部 32、ログインリクエスト生成部 33、ログインリクエスト送信部 34、ブラウザ監視部 35 などから構成されている。

これらの機能部は、後述するブラウザプログラム 56 (図 4) を CPU (Central Processing Unit) 41 で実行することにより、ソフトウェア的に構成される。

#### 【0034】

より詳細には、ブラウザ 10 は、ブラウザ機能部 11 に自動ログイン部 12 をプラグインソフトとして組み込んで構成することもできる。この場合、自動ログイン部 12 を汎用的に使用されているインターネットブラウザの拡張アプリケーションとすることができ、あるいは、自動ログイン部 12 とブラウザ機能部 11 を有するブラウザ 10 をプログラミングすることにより構成してもよい。

#### 【0035】

ブラウザ 10 の、ブラウザ機能部 11 はブラウザ 10 が起動している間中動作する。一方、自動ログイン部 12 は、ICカード RW 21 に非接触 IC カード 7 がセットされている間だけ動作するように構成されている。

以上のように、動作するために、ブラウザ 10 は、ICカード RW 21 に非接触 IC カード 7 がセットされているか否かを監視している。

#### 【0036】

暗号・復号部 31 は、自動ログイン情報 15 の復号化、及び暗号化を行う機能部である。

暗号・復号部 31 は、復号化手段、暗号化手段を構成している。

暗号・復号部 31 は、ICカード RW 21 が非接触 IC カード 7 から読み取った第 1 の鍵情報 9 を取得し、自動ログインサイト情報 16 を復号化する。復号後の自動ログインサイト情報 16 は、RAM などに記憶する。この復号化した自動ログインサイト情報 16 により、ブラウザ 10 は、自動ログインサイト情報 16 を利用できるようになる。

また、暗号・復号部 31 は、第 1 の鍵情報 9 を用いて自動ログインサイト情報 16 を第 1 の鍵情報 9 で復号化可能に暗号化することもできる。これにより、自動ログインサイト情報提供サーバ 4 からダウンロードした最新の自動ログインサイト情報 (暗号化されていない) を暗号化して自動ログイン情報 15 に格納することができる。

#### 【0037】

なお、クライアント端末 3 から自動ログインサイト情報提供サーバ 4 にユーザを特定する情報を提供し (これにより自動ログインサイト情報提供サーバ 4 は、このユーザが使用している第 1 の鍵情報 9 がわかるものとする)、第 1 の鍵情報 9 で復号化可能に暗号化した自動ログインサイト情報 15 を自動ログインサイト情報提供サーバ 4 からクライアント端末 3 に送信するように構成してもよい。この場合は、暗号・復号部 31 に自動ログインサイト情報 16 を暗号化する機能を搭載する必要は必ずしもなくなる。

更に、暗号・復号部 31 は、第 1 の鍵情報 9 と、パスワード入力部 22 から取得した第 2 の鍵情報 (自動ログインパスワード) を用いて自動ログイン個人情報 17 を復号化すると共に、復号化された自動ログイン個人情報 17 をこれらの鍵情報で復号化可能に暗号化することができる。復号化した自動ログイン個人情報 17 は、例えば、RAM (Random Access Memory) などに記憶する。

#### 【0038】

このように、暗号・復号部 31 は、自動ログインサイト情報 16、自動ログイン個人情報 17 を復号化して、他の構成要素からアクセス可能に、RAM などのメモリに記憶することができる。

なお、本実施の形態では、自動ログイン個人情報 17 が第 1 の鍵情報 9 と第 2 の鍵情報の双方を用いて復号化可能としたが、これに限定するものではなく、第 2 の鍵情報により復号化できるように構成してもよい。

#### 【0039】

ブラウザ機能部 11 は、一般の WWW ブラウザと同様に、WWW サーバが提供するサービ

10

20

30

40

50

スをユーザに利用可能に提供する機能部である。

より詳細には、ブラウザ画面（例えば、URL欄を備え、HTMLファイルが定義した解釈した画面を表示する画面）をディスプレイに表示することができ、また、ブラウザ画面上のURL欄に入力してあるURLで特定されるファイルをこのファイルが保存されているWWWサーバからダウンロードする。

所定のファイルには、例えばHTMLファイルやXML（Extensible Markup Language）ファイルなどのマークアップ言語で構成されたものがあり、この場合、ブラウザ機能部11は、これらファイルで定義されている画面をディスプレイに表示する。

ブラウザ機能部11は、サイト選択手段を構成している。

10

#### 【0040】

URL欄には、現在ブラウザ画面に表示されているWebページのURLが表示されており、URLに新たなURLを入力して変更すると、新規入力したURLで特定されるファイルがダウンロードされる。

URL欄へのURLの入力は、ユーザがキーボードから入力することもできる。また、この他に、特定のURLが設定されたアイコンなどのシンボルをブラウザ画面上に配置し、これをユーザがマウス操作でクリックするなどして選択することにより、このアイコンなどに設定されているURLをURL欄に入力することもできる。

#### 【0041】

ブラウザ監視部35は、ブラウザ機能部11のURL欄を監視し、URL欄に入力されているURLが、自動ログインサイト情報16のログインページ情報142（図2）に登録されているURLと一致するか否かを監視している。そして、一致するURLがあった場合、一致したログインページ情報142を特定する特定情報をログインリクエスト生成部33に送る。

20

#### 【0042】

ログインリクエスト生成部33は、ブラウザ監視部35からこの特定情報を受け取り、これを用いてログインリクエストの生成を行う。

ログインリクエスト生成部33は、受け取った特定情報と、ログインページ情報142とをマッチングし、サービス名称141とログインリクエスト情報143を特定する。

#### 【0043】

30

更に、ログインリクエスト生成部33は、特定されたサービス名称141とサービス名称145をマッチングし、ログインリクエスト情報143のパラメータとして設定するパラメータ値（パラメータ値146、147、148、）を取得する。

そして、ログインリクエスト生成部33は、ログインリクエスト情報143と取得したパラメータ値からログインリクエストを生成し、ログインリクエスト送信部34に送る。

ログインリクエストの生成は、ログインリクエスト情報143のパラメータ（%1、%2、）に自動ログイン個人情報17で特定されたパラメータ値を代入する（付属させる）ことにより行う。

#### 【0044】

また、ログインリクエスト生成部33は、自動ログインサイト情報16のサービス名称141に対応する（ひも付けされた）サービス名称145が自動ログイン個人情報17で見つからなかった場合、そのサービス名称141とログインリクエスト情報143を自動追加部32に送る。

40

これは、自動ログインサイト情報16は自動ログインサイト情報提供サーバ4で既に作成されたものであるので、最初にこれに対するパラメータ値をユーザが入力して自動ログイン個人情報17を作成する必要があるためである。

ログインリクエスト生成部33は、自動ログイン情報検索手段、自動ログインサイト情報検索手段、自動ログイン個人情報検索手段、ログインリクエスト生成手段を構成している。

#### 【0045】

50

自動追加部 32 は、ログインリクエスト情報 143 に登録されているが、まだ自動ログイン個人情報 17 に登録されていないサービスサイトに関して、ユーザに自動ログイン個人情報 17 へのパラメータ値の入力を促すと共に、ユーザがログインページで入力したパラメータ値を用いて当該サービスサイトに関する情報を自動ログイン個人情報 17 に追加する。

自動追加部 32 は、この追加を、RAM などに記憶した復号化済みの自動ログイン個人情報 17 に対して行う。そして、後ほど、暗号・復号部 31 は、これを暗号化し、暗号化された自動ログイン個人情報 17 を更新する。

#### 【0046】

より詳細に説明すると、ユーザが自動ログインサイト情報 16 に登録されていて自動ログイン個人情報 17 に登録されていないサービスサイトのログインページにアクセスすると、自動追加部 32 は、「自動ログインに設定しますか？」などといった適当な表示をブラウザ画面に表示し、このログインページが自動ログイン対象であることを知らせる。ここで、ユーザは登録するか否かを選択することができるようになっている。

そして、ユーザが登録を選択した場合、自動追加部 32 は、ユーザがログイン ID やパスワードを入力するためのダイアログを表示し、ユーザからパラメータ値を取得する。

#### 【0047】

あるいは、ログインページ（一般にログイン ID 入力欄やパスワード入力欄などを備えている）でユーザが入力するパラメータ値を観察し、これとログインリクエスト情報 143 とを比較して、どのパラメータにどのパラメータ値（ログイン ID、パスワード）が入力されるかを把握する。そして、自動追加部 32 は、把握したパラメータ値と、ログインリクエスト生成部 33 から受け取ったサービス名称 141 を用いて自動ログイン個人情報 17 を更新することも可能である。自動追加部 32 と暗号・復号部 31 は、自動ログイン個人情報追加手段を構成している。

#### 【0048】

ログインリクエスト送信部 34 は、ログインリクエスト生成部 33 から受け取ったログインリクエストをログインページを送ってきたサーバ 5 に送信する。

本実施の形態では、ログインリクエスト送信部 34 がサーバ 5 にログインリクエストを送信するように構成したが、これに限定するものではなく、例えば、ログインリクエスト送信部 34 からブラウザ機能部 11 にログインリクエストを渡し、ブラウザ機能部 11 からサーバ 5 にログインリクエストを送信するように構成してもよい。

ログインリクエスト生成部 33、ログインリクエスト送信部 34 は、自動ログイン手段を構成している。

#### 【0049】

図 4 は、クライアント端末 3 のハードウェア的な構成の一例を説明するための図である。クライアント端末 3 は、例えばパーソナルコンピュータを用いて構成されており、CPU 41 にバスライン 49 を介して、ROM (Read Only Memory) 42、RAM 43、表示手段 45、入力手段 46、出力手段 47、通信制御手段 48、記憶装置 55、記憶媒体駆動装置 52、入出力 I/F (インターフェース) 51、IC カード RW 21 などの周辺機器が接続して構成されている。

バスライン 49 は、CPU 41 と周辺機器の間で送受信される制御信号やデータ信号の送受信を媒介する。

#### 【0050】

CPU 41 は、後述のブラウザプログラム 56 に従って動作し、サーバ 5 へアクセスしたり、また、自動ログイン処理を行ったりする。また、OS (Operating System) などによって、クライアント端末 3 全体を制御したりなど、各種情報処理や制御を行う。

ROM 42 は、CPU 41 が各種演算や制御を行うための各種プログラム、データ及びパラメータなどを格納した読み取り専用の記憶装置である。CPU 41 は、ROM 42 からプログラムやデータ、パラメータなどを読み込むことはできるが、これらを書き換えたり

10

20

30

40

50

消去したりすることを行わない。

【0051】

RAM43は、CPU41にワーキングメモリとして使用される読み書き可能な記憶装置である。CPU41は、RAM43にプログラムやデータなどを書き込んだり消去したりすることができる。本実施の形態では、RAM43には、復号化された自動ログインサイト情報16や、自動ログイン個人情報17を記憶したり、ログインリクエストを生成したりなどするためのエリアが確保可能となっている。

【0052】

表示手段45は、ブラウザ画面などの表示情報を表示するための手段であり、例えばCRT(Cathode Ray Tube)ディスプレイ、液晶ディスプレイ、プラズマディスプレイなどのディスプレイで構成されている。

10

入力手段46は、例えばキーボードやマウスなどの入力装置から構成されている。

キーボードは、クライアント端末3に対して文字や数字などの情報を入力するための装置である。キーボードは、カナや英文字などを入力するためのキーや数字を入力するためのテンキー、各種機能キー、カーソルキー及びその他のキーによって構成されている。ユーザは、キーボードからURLや、ログインID、パスワードなどを入力することができる。

マウスは、ポインティングデバイスである。GUI(Graphical User Interface)などを用いてクライアント端末3を操作する場合、表示装置上に表示されたボタンやアイコンなどをマウスでクリックすることにより、所定の情報(URLなど)の入力を行うことができる。

20

出力手段47は、例えば印刷装置などの出力装置から構成されている。

【0053】

通信制御手段48は、インターネット6を介してクライアント端末3を自動ログインサイト情報提供サーバ4やサーバ5などに接続するための装置であって、モデム、ターミナルアダプタ、その他の装置によって構成されている。

通信制御手段48はCPU41によって制御され、所定のプロトコルに従ってサーバ5や自動ログインサイト情報提供サーバ4などと信号やデータの送受信を行い、ログインリクエストの送信やサービスサイトが提供する情報を受信したりすることができる。

【0054】

30

記憶媒体駆動装置52は、着脱可能な記憶媒体を駆動してデータの読み書きを行うための駆動装置である。着脱可能な記憶媒体としては、例えば、光磁気ディスク、磁気ディスク、磁気テープ、半導体メモリ、データをパンチした紙テープ、CD-ROMなどがある。なお、CD-ROMや紙テープは、読み込みのみ可能である。

なお、自動ログインサイト情報16は、自動ログインサイト情報提供サーバ4からダウンロードするのではなく、記憶媒体の形で事業者に配布してもらい、記憶媒体駆動装置52を介してクライアント端末3に取り込むこともできる。

【0055】

記憶装置55は、読み書き可能な記憶媒体と、その記憶媒体に対してプログラムやデータを読み書きするための駆動装置によって構成されている。当該記憶媒体として主にハードディスクが使用されるが、その他に、例えば、光磁気ディスク、磁気ディスク、半導体メモリなどの他の読み書き可能な記憶媒体によって構成することも可能である。

40

【0056】

記憶装置55は、ブラウザプログラム56、自動ログインサイト情報データベース57、自動ログイン個人情報データベース58などを記憶している。

CPU41は、記憶装置55の駆動装置を駆動することにより、記憶装置55に対してプログラムやデータの読み込みや書き出しを行うことができる。

記憶装置は、自動ログイン情報記憶手段を構成している。

【0057】

ブラウザプログラム56は、CPU41にブラウザ機能を発揮させるためのプログラムで

50

ある。ブラウザプログラム 56 が CPU 41 に読み込まれて実行されることにより、図 3 に示した暗号・復号部 31 からブラウザ監視部 35、及びブラウザ機能部 11 の各構成要素がソフトウェア的に構成される。

自動ログインサイト情報データベース 57 と、自動ログイン個人情報データベース 58 は、それぞれ暗号化された自動ログインサイト情報 16、自動ログイン個人情報 17 を格納するデータベースである。

#### 【0058】

自動ログインサイト情報データベース 57 に格納する自動ログインサイト情報 16 は、通信制御手段 48 を介して自動ログインサイト情報提供サーバ 4 からダウンロードしたものである。

図示しないが、記憶装置 55 には、例えば、通信制御手段 48 を制御し、クライアント端末 3 とネットワークでつながれた端末装置やサーバ装置との通信を維持する通信プログラムや、メモリ管理や入出力管理などのクライアント端末 3 を動作させるための基本ソフトウェアである OS、及び IC カード RW 21 のドライバソフトなどの各種プログラムや、その他のデータが記憶されている。

#### 【0059】

入出力 I/F 51 は、例えば、シリアルインターフェースやその他の規格のインターフェースにより構成されている。入出力 I/F 51 に当該インターフェースに対応した外部機器を接続することにより、クライアント端末 3 の機能を拡張することができる。このような外部機器として例えば、ハードディスクなどの記憶装置、スピーカ、マイクロフォンなどがある。

IC カード RW 21 は、非接触 IC カード 7 とデータの送受信を行ったり、非接触 IC カード 7 に電力を供給するアンテナが備えられている。

#### 【0060】

本実施の形態では、クライアント端末 3 は、例えば、パーソナルコンピュータで構成されているが、これに限定するものではなく、インターネット接続機能を持った情報家電（テレビ、CE 機器）など、各種のハードウェアで構成することができる。

例えば、インターネット接続機能を持ったテレビの場合、テレビ画面が表示手段 45 を構成し、赤外線式のリモートコントローラが入力手段 46 を構成する。

ユーザは、テレビ画面に表示されたブラウザ画面を見ながら、リモートコントローラで情報を入力する。

#### 【0061】

図 5 は、ブラウザ 10 が自動ログインを行う手順を説明するためのフローチャートである。

なお、以下のフローチャートで各構成要素が行う動作は、CPU 41 がブラウザプログラム 56 に従って動作することにより実現されるものである。

ここで、非接触 IC カード 7 は、IC カード RW 21 にまだセットされておらず、自動ログインサイト情報 16、自動ログイン個人情報 17 の何れもまだ復号化されていないものとする。

#### 【0062】

ブラウザ 10 は、IC カード RW 21 に非接触 IC カード 7 がセットされているか否かを監視しており、非接触 IC カード 7 がセットされると、自動ログイン部 12 を起動する（ステップ 1100）。そして、暗号・復号部 31 は、第 1 の鍵情報 9 を非接触 IC カード 7 から取得して自動ログインサイト情報 16 を復号化し、RAM 43 に記憶する。更に、ブラウザ監視部 35 が、ブラウザ機能部 11 を監視し始め、ブラウザ画面の URL 欄に入力される値をチェック（確認）する（ステップ 1200）。

なお、ブラウザ 10 は、非接触 IC カード 7 が IC カード RW 21 にセットしてある間も、一定時間毎に非接触 IC カード 7 がセットされているか否かを監視しており、非接触 IC カード 7 が IC カード RW 21 から取り外されると、自動ログイン部 12 の機能を終了させる。

10

20

30

40

50

## 【0063】

次に、ユーザは、ホームページ上のクリックボタン（ログインページにジャンプするように設定されているもの）をクリックするなどしてログインページにアクセスする（ステップ1105）。これに対して、サーバ5は、ログインページをクライアント端末3に送信する（ステップ1300）。

図6（a）は、ユーザがログインページを要求する際に、ブラウザ画面に表示されるホームページの一例を示したものである。

ユーザは、サービスAを提供するサービスサイトにアクセスし、ページ101を表示させ、ログインボタン102をクリックすると、サーバ5からログインページが送信されてくる。ブラウザ10がログインページを受け取ると、URL欄にログインページのURLが入力される。

10

ここで、このログインページは自動ログインサイト情報16で登録されているものであるとする。

## 【0064】

図5に戻り、自動ログイン部12は、URL欄に入力された値をチェックし（ステップ1205）、これがログインページ情報142に登録されたURLにマッチングするので、ブラウザ画面上にこのサービスサイトが自動ログイン対象である旨の自動ログイン可能通知を行う（ステップ1110）。

図6（b）は、自動ログイン可能通知の一例を示した図である。

ログインページ105は、サーバ5がログイン処理するためのログインIDを入力するログインID入力欄106と、パスワードを入力するためのパスワード入力欄107を備えている。これらは、サーバ5がクライアント端末3に送信した画面データにより構成されたものである。そして、これらの欄の上に、「ICカードで自動ログインできます。」といった自動ログイン可能通知が表示されている。この部分は、自動ログイン部12がブラウザ機能部11に表示させたものである。

20

ユーザは、ログイン通知により、これからログインしようとしているサービスサイトが自動ログイン対象であることを知ることができる。

## 【0065】

図5に戻り、ブラウザ機能部11は、自動ログイン可能通知した後、自動ログインパスワード入力画面を表示し、自動ログインパスワードの入力をユーザに促す。そして、ユーザがパスワード入力部22から自動ログインパスワードを入力すると（ステップ1115）、自動ログイン部12がこれを取得し、これが正しいものであるか否かを照合する（ステップ1210）。なお、照合用の自動ログインパスワードは、予め記憶装置55やROM42などに格納しておく。

30

ここでは、自動ログインパスワードは正常に照合されたものとする。

## 【0066】

図6（c）は、自動ログインパスワード入力画面の一例を示した図である。図に示したように、自動ログインパスワード入力画面110では、「自動ログイン用のパスワードを入力してください。」などと、自動ログインパスワードの入力をユーザに促す表示が行われると共に、自動ログインパスワード入力欄111が表示される。ユーザが自動ログインパスワード入力欄111に自動ログインパスワードを入力して例えば、リターンキーを押し下げると自動ログイン部12が、入力された自動ログインパスワードの照合を行う。

40

## 【0067】

図5に戻り、自動ログインパスワードが適切に照合されると、暗号・復号部31は、第1の鍵情報9と、第2の鍵情報（自動ログインパスワード）を用いて自動ログイン個人情報17を復号化し、RAM43に記憶する（ステップ1215）。

本実施の形態では、一旦RAM43に記憶した自動ログイン個人情報17は、自動ログイン部12の動作を終了するまで保たれるものとする。なお、自動ログインする毎に、自動ログインパスワードをその都度ユーザに入力してもらい、自動ログイン個人情報17の復号化、及びRAM43上の自動ログイン個人情報17の消去を、その都度行うようにして

50

セキュリティを高めてもよい。

次に、ログインリクエスト生成部 33 がユーザが自動ログインで使用しているサービスサイト用のパラメータ値を自動ログイン個人情報 17 で確認し（ステップ 1220）、自動ログインサイト情報 16 と自動ログイン個人情報 17 を用いてログインリクエストを生成する。そして、そのログインリクエストをログインリクエスト送信部 34 がサーバ 5 に送信する（ステップ 1225）。

【0068】

次に、サーバ 5 は、クライアント端末 3 から送信されてきたログインリクエストを受信し、ログイン処理を開始する（ステップ 1305）。そして、サーバ 5 は、ユーザのログイン認証がなされると、ログイン認証後の画面データをクライアント端末 3 に送信する（ステップ 1310）。

10

クライアント端末 3 では、ブラウザ機能部 11 がサーバ 5 から送信されてきたログイン後画面データを用いてログイン後画面を表示する（ステップ 1120）。

【0069】

図 6（d）は、ログインリクエスト送信部 34 がログインリクエストを送信した後、ログイン後画面を表示するまでの間、ブラウザ画面に表示されるログイン中画面の一例を示したものである。ユーザは、ログイン中画面 113 により、現在自動ログインを行っていることを知ることができる。

図 6（e）は、ログイン後画面の一例を示した図である。ログイン後画面 115 は、占いサービスを提供するサービスサイトの画面であって、クリックボタン 116 をクリックすると、ユーザの生年月日、星座、名前などの数によって判断されたユーザの運勢が表示される。

20

なお、RAM 43 に記憶した復号後の自動ログイン情報 15 は、自動ログイン部 12 の動作を終了すると消去されるようになっている。

【0070】

図 7 は、既に非接触 IC カード 7 が IC カード RW 21 にセットされており、自動ログインパスワードも入力され、自動ログインサイト情報 16、自動ログイン個人情報 17 の何れもが復号化されている場合のブラウザ 10 の動作を説明するためのフローチャートである。これは、例えば、自動ログイン部 12 を起動してから 2 回目以降に自動ログインする場合などが該当する。

30

図 5 と重複する部分については説明を簡略化する。

自動ログイン部 12 は、自動ログインサイト情報 16 を用いてブラウザ機能部 11 を監視している（ステップ 2200）。

ユーザがログインページにアクセスすると（ステップ 2100）、サーバ 5 はログインページをクライアント端末 3 に送信する（ステップ 2300）。

【0071】

クライアント端末 3 では、ログインページを受信すると、ブラウザ監視部 35 が URL をチェックする（ステップ 2205）。ここでは、このログインページが自動ログインの対象であったとする。

すると、ログインリクエスト生成部 33 は、自動ログイン個人情報 17（既に RAM 43 に記憶してある）で、このログインリクエスト情報 143 用のパラメータ値が存在することを確認する（ステップ 2210）。ここでは、ログインリクエスト情報 143 用のパラメータ値が存在するものとする。

40

次に、ログインリクエスト生成部 33 がログインリクエストを生成し、ログインリクエスト送信部 34 がこれをサーバ 5 に送信する（ステップ 2215）。

【0072】

サーバ 5 では、クライアント端末 3 からログインリクエストを受信してログイン処理を行い（ステップ 2305）、ログイン後ページの画面データをクライアント端末 3 に送信する（ステップ 2310）。

クライアント端末 3 は、この画面データを受信し、ブラウザ機能部 11 がログイン後ペー

50

シを表示する（ステップ2105）。

【0073】

この例では、自動ログインサイト情報16と、自動ログイン個人情報17が既に復号化されてRAM43に記憶されているため、ユーザが自動ログインパスワードを入力する手間を省略することができる。

そのため、自動ログイン部12を立ち上げて、2回目以降に自動ログイン対象のサービスサイトにログインする場合は（1回目は、自動ログインパスワードを入力する必要がある）、自動ログインパスワードを入力しないで済む。

【0074】

図8は、自動ログインサイト情報16に対応する情報が自動ログイン個人情報17にない場合に、自動追加部32が自動ログイン個人情報17を更新する場合の、ブラウザ10の動作を説明するための図である。

現在、自動ログイン部12が起動されていないものとする。

まず、ユーザが非接触ICカード7をICカードRW21にセットし、自動ログイン部12を起動する（ステップ3100）。

すると、暗号・復号部31が自動ログインサイト情報16、自動ログイン個人情報17を復号化すると共に、ブラウザ監視部35がブラウザ機能部11の監視を開始する（ステップ3200）。

【0075】

ユーザがログインページにアクセスすると（ステップ3105）、サーバ5は、ログインページをクライアント端末3に送信する（ステップ3300）。

次に、ブラウザ監視部35がこのログインページが自動ログインの対象であることをURLでチェックし（ステップ3205）、ログインページと自動ログイン可能通知を表示する（ステップ3110）。

【0076】

ユーザが自動ログインパスワード入力欄から自動ログインパスワードを入力すると（ステップ3115）、自動ログイン部12は、この自動ログインパスワードを照合し（ステップ3210）、暗号・復号部31が自動ログイン個人情報17を復号化する（ステップ3215）。

次に、ログインリクエスト生成部33が、このログインページに対応する情報が自動ログイン個人情報17に存在するか否かを確認し、対応する情報が自動ログイン個人情報17に存在しないことを確認する（ステップ3220）。

すると、自動追加部32がユーザに適切なパラメータ値（ログインID、パスワードなど）を入力するためのダイアログをブラウザ機能部11に表示させ（ステップ3225）、ユーザがこれに対してパラメータ値を入力する（ステップ3120）。

ここで、このダイアログは、サーバ5が送信してきたログインページを用いることもできる。この場合、自動追加部32は、ユーザがログインページで入力したパラメータ値を取得する。

【0077】

次に、自動追加部32は、取得したパラメータ値を用いて自動ログイン個人情報17を更新する（ステップ3230）。

そして、ログインリクエスト生成部33が更新された自動ログイン個人情報17を用いてログインリクエストを生成し、ログインリクエスト送信部34がこのログインリクエストをサーバ5に送信する（ステップ3235）。

【0078】

サーバ5は、クライアント端末3からログインリクエストを受信し、これを用いてログイン処理を行い（ステップ3305）、ログイン後ページの画面データをクライアント端末3に送信する（ステップ3310）。クライアント端末3では、ブラウザ機能部11がこのログイン後ページの画面データを用いてログイン後画面を表示する（ステップ3125）。

10

20

30

40

50



一方、暗号・復号部 31 は、更新された自動ログイン個人情報 17 を暗号化する（ステップ 3240）。

【0079】

図 9 は、ユーザが URL 欄に、直接ログインページの URL を入力した場合の動作を説明するためのフローチャートである。即ち、図 5 などのフローチャートの例は、サーバ 5 が送信してきたログインページを受信し、それからこのログインページの URL が得られるのに対し、図 9 の例は、ユーザがログインページの URL を URL 欄に直接入力したり、アイコン化したログインページをクリックして URL 欄にログインページの URL を入力する場合の例である。

まず、非接触 IC カード 7 を IC カード RW 21 にセット、自動ログイン部 12 を起動する（ステップ 4100）。

次に、暗号・復号部 31 が第 1 の鍵情報 9 を用いて自動ログインサイト情報 16 を復号化すると共に、ブラウザ監視部 35 がブラウザ機能部 11 の監視を開始する（ステップ 4200）。

【0080】

ユーザが、ブラウザ画面の URL 欄にログインページの URL を入力すると（ステップ 4105）、ブラウザ監視部 35 がこれをチェックする（ステップ 4205）。そしてブラウザ機能部 11 が自動ログイン可能通知を行い（ステップ 4110）、更に、自動ログインパスワード入力欄を表示する。ユーザが自動ログインパスワードを入力すると（ステップ 4115）、自動ログイン部 12 は、この自動ログインパスワードの照合を行う（ステップ 4210）。照合が適切に行われると、暗号・復号部 31 が自動ログイン個人情報 17 を復号化する（ステップ 4215）。

【0081】

次に、ログインリクエスト生成部 33 が、このログインページに対応する情報が自動ログイン個人情報 17 にあることを確認する（ステップ 4220）。

そして、ログインリクエスト生成部 33 がログインリクエストを生成し、ログインリクエスト送信部 34 がこれをサーバ 5 に送信する（ステップ 4225）。

サーバ 5 は、このログインリクエストを用いてログイン処理を行い（ステップ 4300）、ログイン後ページの画面データをクライアント端末 3 に送信する（ステップ 4305）。

クライアント端末 3 では、ブラウザ機能部 11 が、この画面データを用いてログイン後ページを表示する（ステップ 4120）。

【0082】

図 10 は、既に、自動ログインサイト情報 16、自動ログイン個人情報 17 が復号化されており、ユーザが URL 欄に直接ログインページの URL を入力する場合の動作を説明するためのフローチャートである。

まず、ブラウザ監視部 35 は、ブラウザ機能部 11 を監視している（ステップ 5200）。

次に、ユーザが URL 欄にログインページの URL を入力すると（ステップ 5100）、ブラウザ監視部 35 がこの URL が自動ログインサイト情報 16 で登録されていることをチェックし（ステップ 5205）、更にこれに該当する情報が自動ログイン個人情報 17 にあることを確認する（ステップ 5210）。

【0083】

次に、ログインリクエスト生成部 33 がログインリクエストを生成し、ログインリクエスト送信部 34 がこのログインリクエストをサーバ 5 に送信する（ステップ 5215）。

サーバ 5 は、このログインリクエストを受信し、ログイン処理を行い（ステップ 5300）、ログイン後ページの画面データをクライアント端末 3 に送信する（ステップ 5305）。

クライアント端末 3 では、ブラウザ機能部 11 がこの画面データを用いてログイン後ページを表示する（ステップ 5105）。

10

20

30

40

50

## 【0084】

図11は、自動ログイン情報の他の形態を説明するための図である。この例の自動ログイン情報150は、自動ログインサイト情報16と自動ログイン個人情報17に区別されておらず、サービス名称、ログインページ情報、ログインリクエスト情報、パラメータが1つの単位としてサービス名称毎に管理されている。

この自動ログイン情報は、例えば、第1の鍵情報9及び第2の鍵情報で復号化可能に暗号化されている。

この場合、ICカードRW21に非接触ICカード7をセットすると共に、パスワード入力部22から自動ログインパスワードを入力して自動ログイン情報が復号化され、自動ログイン部12が動作するようになる。

## 【0085】

図12は、自動ログイン情報の更に他の形態を説明するための図である。

この形態の自動ログイン情報は、自動ログイン情報160と、自動ログイン個人情報161から構成されている。

ログインを要するサービスサイトは、例えば、銀行預金の管理など秘匿性の高いサイトもあれば、占いサイトのように他者に自動ログイン個人情報が漏れても被害の小さいものまで各種ある。ここでは、自動ログイン個人情報161に登録されている情報の重要度をユーザが判断し、重要度の低いものを自動ログイン情報160に登録するようにする。

## 【0086】

自動ログイン情報160は、第1の鍵情報9で復号化可能に暗号化されている。また、自動ログイン個人情報161は、第1の鍵情報9、及び第2の鍵情報で復号化可能に暗号化されている。

自動ログイン情報160は、サービス名称、ログインページ情報、ログインリクエスト情報、パラメータ値などから構成され、自動ログイン個人情報161は、サービス名称、パラメータ値などから構成されている。

そして、自動ログイン情報160と自動ログイン個人情報161は、サービス名称で互い付けされている。

## 【0087】

ユーザは、自動ログイン個人情報161に登録されている情報のうち、所望のサービスに関するものだけ、自動ログイン情報160に登録することができる。

例えば、図に示した自動ログイン情報160では、サービスA、B、Eにパラメータ値が登録され、サービスC、Dには登録されていない。

ログインリクエスト生成部33は、自動ログイン情報160を用いてログインリクエストを生成するように構成されており、パラメータ値が登録されていないものに関しては、ログインリクエストを生成しない。

## 【0088】

ユーザは、自動ログインの対象となっているサービスサイトのうち、自動ログイン情報160に自動ログイン個人情報161に登録してある情報を登録するか否かを判断し、登録してよいと判断した情報を自動ログイン個人情報161から自動ログイン情報160に登録する。

自動ログイン個人情報161は、自動追加部32によって更新されるが、ユーザは、これを自動ログインに使用するか否かを選択することができる。

## 【0089】

なお、本実施の形態では、ICカードRW21で非接触ICカード7がセットされているか否かを一定時間毎にチェックしているが、これを用いて非接触ICカード7がセットされていない場合にクライアント端末3をロックするように構成することもできる。

このロック機構の形態は各種考えられるが、例えば、非接触ICカード7がICカードRW21から取り外されている間、ディスプレイのスクリーンセーバを強制的に表示し、更に、キーボードやマウスなどからの入力を受け付けないようにすることができる。そして、クライアント端末3の状態は、非接触ICカード7が取り外された時点の状態に保存す

10

20

30

40

50

れる。

【0090】

また、あるユーザがクライアント端末3にログインした場合、そのユーザがログアウトするまで、そのユーザの非接触ICカード7でのみロック状態を解除できるように構成することもできる。即ち、クライアント端末3にログインした状態で、そのユーザが非接触ICカード7と共に席を外すなどしてクライアント端末3をロック状態にした場合、他のユーザが自分の非接触ICカード7をセットしてもそのロック状態を解除することはできない。

【0091】

この場合に、クライアント端末3は、他のユーザからの入力を受け付けない一方、ロック前に行っていた処理をロック中に続行するように構成することもできる。

10

例えば、数値計算を長時間に渡って行っている場合、クライアント端末3をロック状態にし、外部からの入力は受け付けないが、内部での数値計算は引き続き行うように設定することができる。このように構成することにより、数値計算中に、他のユーザが誤って処理を中断してしまうなどのアクシデントを防止することができる。

【0092】

また、ICカードRW21にセットされている非接触ICカード7を検出することにより、クライアント端末3におけるユーザの着席状況を把握することもできる。

例えば、社内にある多数のクライアント端末3のうち、何れのクライアント端末3をどの社員が利用しているかということ进行管理することができる。

20

【0093】

以上に述べた第1の実施の形態により、以下のような効果を得ることができる。

(1) ユーザがネットワーク(インターネット6など)を介してサーバが提供するサービスサイトにログインする際に、そのサービスサイトに対して設定したユーザID、パスワードを入力することなく、非接触ICカード7などの記憶媒体を用いてログイン情報を読み込むことにより、ログインリクエストの生成、送信を自動化し、利便性、安全性、保守性の優れた自動ログインシステムを提供することができる。

(2) ユーザは、自動ログインシステム1を利用することにより、従来キーボードなどから入力していたユーザIDとパスワードを入力する手間を省き、負荷が軽減されるだけでなく、あらゆるインターネット6上のサービスサイトへのログインも自動で行えるなど、利便性の高い自動ログインシステム1を利用できる。

30

【0094】

(3) 各サービスサイトへのログインには、非接触ICカード7と自動ログインパスワードが必要となり、非接触ICカード7を所持し、かつ、自動ログインパスワードを知るものの以外はログインすることができないため、非接触ICカード7が第三者の手に渡っても悪用されることはない。

(4) キーボードからの入力の負担が軽減されているため、サービスへのログインIDやパスワードなどは最大長で複雑なものを使用することができる。そのため、第三者がログインIDやパスワードを盗用し、解読して悪用されることが困難となり、セキュリティ性、安全性が高い自動ログインシステム1を利用することができる。

40

【0095】

(第2の実施の形態)

図13は、本発明の第2の実施の形態に係る自動ログインシステム1aの構成を説明するための図である。

第1の実施の形態と同じ構成要素に関しては同じ符号を付すものとし、説明を省略する。

また、第1の実施の形態に対応する構成要素には、同じ符号に添え字aを付して示す。

第1の実施の形態では、クライアント端末3は、自動ログインサイト情報16を自動ログインサイト情報提供サーバ4からダウンロードしたが、本実施の形態では、クライアント端末3でこれを作成する。

【0096】

50

クライアント端末 3a は、ブラウザ 10a を備えている。ブラウザ 10a は、ブラウザ機能部 11 と自動ログイン部 12a から構成されている。

自動ログイン部 12a は、第 1 の実施の形態の自動ログイン部 12 と同様の機能に加え、図示しないが、自動ログインサイト情報 16 を生成・更新する自動ログインサイト情報生成部を備えている。

自動ログイン情報 15 の構成は第 1 の実施の形態と同じであるが、本実施の形態の自動ログインサイト情報 16 は、自動ログインサイト情報生成部が生成する。

【0097】

本実施の形態のブラウザ監視部 35 は、第 1 の実施の形態と同様にブラウザ画面の URL 欄に入力された情報が、ログインページ情報 142 に一致するか監視しているが、一致しなかった場合は、更に自動ログインサイト情報生成部が、この入力された情報がログインページの URL であるか否かを判断する。この判断は、例えば、「login」といったログインページの URL に使われる頻度の高い文字列が含まれるか否かを判断する。このように、URL 欄に入力された情報で、ログインページ情報 142 に一致せず、「login」などの文字列を含む情報は、未登録のログイン情報であると推定される。

【0098】

自動ログインサイト情報生成部は、ユーザが未登録のログインページにアクセスした場合、ユーザにダイアログを表示してパラメータ値を入力してもらったか、ログインページにユーザが入力した情報を記憶しておくなどして（即ち、どのパラメータにどのようなパラメータ値を入力したか）、これを用いて各種情報を自動ログインサイト情報 16 と自動ログイン個人情報 17 に登録する。

なお、上の例では、未登録のログインページを自動検出するように設定したが、ユーザが手動で設定するようにしてもよい。即ち、ユーザが未登録のログインページにアクセスした場合、ユーザが自動ログインサイト情報生成部を手動で起動し、自動ログインサイト情報 16、自動ログイン個人情報 17 を更新するように構成することもできる。

【0099】

図 14 は、自動ログインサイト情報などを自動更新する場合のブラウザ 10 の動作を説明するためのフローチャートである。

まず、非接触 IC カード 7 を IC カード RW 21 にセットして自動ログイン部 12a を起動する（ステップ 6100）。

そして、暗号・復号部 31 が自動ログインサイト情報 16 を復号化し、これを用いてブラウザ監視部 35 がブラウザ機能部 11 の監視を開始する（ステップ 6200）。

【0100】

次に、ユーザがブラウザ機能部 11 からログインページにアクセスする（ステップ 6105）。ここで、アクセスするログインページは、自動ログインサイト情報 16 に登録されていないものであるとする。

次に、サーバ 5 は、ログインページの画面データをクライアント端末 3 に送信する（ステップ 6300）。

クライアント端末 3 はこの画面データを受信し、自動ログインサイト情報生成部が、このログインページが新規（未登録）のものであることを検出する（ステップ 6205）。

【0101】

すると、自動ログインサイト情報生成部は、ブラウザ機能部 11 にダイアログを表示させ（ステップ 6210）、ユーザにパラメータを入力してもらった（ステップ 6110）。

次に、自動ログイン部 12a は、自動ログインパスワード入力ダイアログをブラウザ機能部 11 に表示させ（ステップ 6215）、ユーザに自動ログインパスワードを入力してもらった（ステップ 6115）。

自動ログイン部 12a は、自動ログインパスワードの正当性を照合し（ステップ 6220）、自動ログインパスワードが適当であった場合、暗号・復号部 31 が自動ログイン個人情報 17 を復号化する。

【0102】

10

20

30

40

50

次に、ログインリクエスト生成部 83 が、ログインページの画面データとユーザが入力したパラメータ値を用いてログインリクエストを生成し、サーバ 5 に送信する（ステップ 6225）。

これに対して、サーバ 5 は、ログイン処理し（ステップ 6305）、ログイン後ページの画面データをクライアント端末 3 に送信する（ステップ 6310）。

クライアント端末 3 では、ブラウザ機能部 11 がこの画面データを用いてログイン後ページを表示する（ステップ 6120）。

一方、自動ログインサイト情報生成部は、自動ログインサイト情報 16 と自動ログイン個人情報 17 に、新たに追加された内容を加えて更新し、これを暗号・復号部 31 が暗号化する（ステップ 6230）。

本実施の形態では、クライアント端末 3 側で自動ログイン情報を更新することができる。

【0103】

（第 3 の実施の形態）

図 15 は、第 3 の実施の形態に係る自動ログインシステム 1 b のシステム構成の一例を示した図である。

第 1 の実施の形態と同様な構成要素には同じ符合を付し、説明を省略する。また、第 1 の実施の形態に対応する構成要素には、同じ符合に添え字 b を付して示す。

本実施の形態は、インターネット 6 を介して提供される個々のサービスへのログイン認証を非接触 IC カード 7 b からログイン情報を読み込むことにより、自動的にログインするものである。

【0104】

本実施の形態では、自動ログイン情報 15 b を非接触 IC カード 7 b に格納する。なお、図示しないが、自動ログインパスワードも暗号化して格納しておく。これは、自動ログイン部 12 b で復号化し、ユーザがパスワード入力部 22 から入力した自動ログインパスワードを照合する際に利用する。

自動ログイン情報 15 b には、自動ログインサイト情報 16 と自動ログイン個人情報 17 の両方を記憶させてもよいし、何れか一方を非接触 IC カード 7 b に記憶し、他方をクライアント端末 3 b で記憶するように構成してもよい。

【0105】

何れか一方を非接触 IC カード 7 b に記憶させる場合、自動ログイン個人情報 17 を非接触 IC カード 7 b に記憶させ、自動ログインサイト情報 16 をクライアント端末 3 b で記憶させるようにすると、自動ログイン機能を持つ同様なブラウザ 10 を備えた他のクライアント端末 3 b で、非接触 IC カード 7 b をセットすることにより、同様に自動ログインを行うことができる。

また、自動ログインサイト情報 16、自動ログイン個人情報 17 の双方を非接触 IC カード 7 b に記憶させても同様に、他のクライアント端末 3 b から自動ログインすることができる。

第 1 の実施の形態では、暗号・復号部 31 は、記憶装置 55 に対してアクセスし、自動ログイン情報 15 の復号化、及び暗号化を行ったが、本実施の形態では、暗号・復号部 31 は、IC カード RW 21 を介して、非接触 IC カード 7 b にアクセスし、自動ログイン情報 15 b の復号化、及び暗号化を行う。

【0106】

自動ログイン情報 15 b は、暗号化したままファイルとしてクライアント端末 3 b の RAM 43 などへ書き出すことができるようになっており、自動ログイン部 12 b は、このファイルを用いて自動ログインすることができる。また、自動ログイン情報 15 b は非接触 IC カード 7 b と共に携帯可能であるため、ユーザは、他のクライアント端末 3 b から自動ログインすることができる。

このように、本実施の形態では、非接触 IC カード 7 b を用いることにより、ブラウザ 10 を備えた複数のクライアント端末 3 b からの自動ログインが可能となる。

【0107】

10

20

30

40

50

また、各サービスサイトへのログインには、非接触ＩＣカード７ｂと自動ログインパスワードが必要となり、非接触ＩＣカード７ｂに格納されているユーザ認証用のパスワード情報を知るもの意外はログインすることができないため、ＩＣカードが第三者の手に渡っても悪用されることはない。

更に、非接触ＩＣカード７ｂを利用可能とするパスワードを設定し、このパスワードを入力しないと、クライアント端末３ｂから自動ログイン情報１５ｂにアクセスできないよう構成すると、更にセキュリティを高めることができる。この場合、クライアント端末３ｂは、ユーザが非接触ＩＣカード７ｂをＩＣカードＲＷ２１にセットしたときに、パスワードを入力するように求めるようにする。

また、このパスワードを自動ログインパスワードとすると、ユーザは１つのパスワードだけ記憶しておけばよく、ユーザの負担を軽減することができる。

【０１０８】

（第４の実施の形態）

図１６は、第４の実施の形態に係る自動ログインシステム１ｃのシステム構成の一例を示した図である。

第１の実施の形態と同様な構成要素には同じ符号を付し、説明を省略する。また、第１の実施の形態に対応する構成要素には、同じ符号に添え字ｃを付して示す。

本実施の形態では、自動ログイン情報を着脱可能な記憶媒体に格納し、ユーザが携帯できるようにする。

第３の実施の形態では、非接触ＩＣカード７ｂが第三者に渡った場合、第１の鍵情報９と自動ログイン情報１５ｂが共にこの第三者に渡ってしまうが、本実施の形態は、自動ログイン情報１５ｃを非接触ＩＣカード７とは別に管理するため、セキュリティが高まる。

【０１０９】

本実施の形態のクライアント端末３ｃは、記憶媒体１９ｃが着脱可能なスロット１８ｃを備えている。スロット１８ｃは、例えば、入出力Ｉ／Ｆ５１（図４）に接続されており、スロット１８ｃにセットされた記憶媒体１９ｃに対してＣＰＵ４１が自由にデータの読み書きを行えるようになっている。

記憶媒体１９ｃは、例えば、不揮発性の半導体メモリであり、この他に、磁気記憶媒体や光ディスクなど、他の形態の記憶媒体を用いることも可能である。

【０１１０】

記憶媒体１９ｃには、自動ログインサイト情報１６と自動ログイン個人情報１７からなる自動ログイン情報１５ｃが記憶されており、暗号・復号部３１は、スロット１９ｃを介して、自動ログイン情報１５ｃを復号化、及び暗号化する。

このため、記憶媒体１９ｃをクライアント端末３ｃと同様な構成を持ったクライアント端末３ｃ'のスロット１８ｃ'にセットすることにより、ユーザはクライアント端末３ｃと同様に自動ログインすることができる。

なお、図示しないが、記憶媒体１９ｃに自動ログインパスワードも暗号化して格納しておく。これは、自動ログイン部１２ｃで復号化し、ユーザがパスワード入力部２２から入力した自動ログインパスワードを照合する際に利用する。

【０１１１】

以上に述べた本実施の形態では、自動ログイン情報１５ｃが自動ログインサイト情報１６と自動ログイン個人情報１７から構成されているとしたが、これに限定するものではなく、例えば、自動ログインサイト情報１６をクライアント端末３ｃに記憶させ、自動ログイン個人情報１７を記憶媒体１９ｃに記憶させるようにしてもよい。

この場合、クライアント端末３ｃ'に自動ログインサイト情報１６を記憶させておけば、記憶媒体１９ｃに記憶された自動ログイン個人情報１７を用いてクライアント端末３ｃ'から自動ログインすることができる。

【０１１２】

本実施の形態では、非接触ＩＣカード７と記憶媒体１９ｃを用いることにより、ブラウザ１０を備えた複数のクライアント端末３ｃからの自動ログインが可能となる。

10

20

30

40

50

また、各サービスサイトへのログインには、非接触ＩＣカード７と自動ログインパスワード、及び記憶媒体１９ｃが必要となり、記憶媒体１９ｃに格納されている自動ログインパスワードを知るもの以外はログインすることができないため、非接触ＩＣカード７や記憶媒体１９ｃが第三者の手に渡っても濫用されることはない。

#### 【０１１３】

以上、本発明のいくつかの実施形態について説明したが、本発明は説明した実施形態に限定されるものではなく、各請求項に記載した範囲において各種の変形を行うことが可能である。

例えば、以下のように構成することもできる。

(１) カードを識別する識別番号を保持するカードと、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報と、前記サービスサイトにログインするための個人情報とを格納する記録媒体と、を用いて複数サイトへログインするクライアント端末において、前記カードの識別番号によって、前記記録媒体から前記ログインサイト情報を読み出すログインサイト情報読み出し手段と、前記個人情報を読み出す際に必要となるパスワードを要求する要求手段と、前記パスワードによって、前記個人情報を読み出す個人情報読み出し手段と、前記ログインサイトに対応する前記個人情報をを用いて、自動ログインすることの特徴とするクライアント端末。

(２) カードを識別する識別番号を保持するカードを用いて複数サイトへログインするクライアント端末において、前記カード内に格納される情報を読み出す読み出し手段と、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報を格納するログインサイト情報記憶手段と、前記サービスサイトへログインするための個人情報を登録する登録手段と、前記個人情報を格納する個人情報記憶手段とを備えるクライアント端末であって、前記カードの識別番号によって、前記ログインサイト情報記憶手段に格納される前記ログインサイト情報を読み出すことを可能とすることを特徴とする。

(３) 前記個人情報を読み出す場合には、パスワードを要求する要求手段を更に備えることを特徴とする上記(１)、(２)に記載のクライアント端末。

(４) 前記ログインサイト情報には、ログインサイトのＵＲＬが含まれることを特徴とする上記(２)に記載のクライアント端末。

(５) 前記要求手段によって得られたパスワードによって、前記ログインサイト情報に対応する個人情報を読み出し、自動的にログインすることを特徴とする上記(３)に記載のクライアント端末。

(６) 前記カードは、非接触カードであることを特徴とする上記(２)に記載のクライアント端末。

(７) 前記カードを識別する識別番号を保持するカードを用いて複数サイトへログインするログイン方法において、自動ログイン可能な少なくとも１つ以上のサービスサイトに関するログインサイト情報を格納するステップと、前記サービスサイトへログインするための個人情報を登録するステップと、前記個人情報を、対応する前記ログインサイト情報と対応付けて格納するステップと、前記カードの識別番号によって、前記ログインサイト情報を読み出すステップと、前記個人情報を読み出すために、パスワードを要求するステップと、前記個人情報をを用いて前記ログインサイトにログインすることを特徴とするログイン方法。

#### 【０１１４】

##### 【発明の効果】

本発明の自動ログインシステムなどによれば、セキュリティ面で安全性を高めることができると共に、各サイトへのログイン操作の負担を軽減することができる。

##### 【図面の簡単な説明】

【図１】本実施の形態のシステム構成を説明するための図である。

【図２】自動ログイン情報の論理的な構成の一例を示した図である。

【図３】ブラウザの機能的な構成を説明するための模式図である。

【図４】クライアント端末のハードウェア的な構成の一例を説明するための図である。

10

20

30

40

50

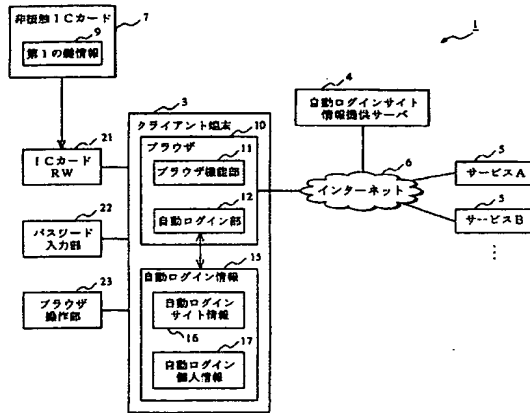
- 【図 5】ブラウザが自動ログインを行う手順を説明するためのフローチャートである。
- 【図 6】自動ログインの際にブラウザ画面に表示される画面の一例を示した図である。
- 【図 7】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
- 【図 8】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
- 【図 9】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
- 【図 10】ブラウザが自動ログインを行う他の手順を説明するためのフローチャートである。
- 【図 11】自動ログイン情報の他の形態を説明するための図である。
- 【図 12】自動ログイン情報の更に他の形態を説明するための図である。
- 【図 13】本発明の第 2 の実施の形態に係る自動ログインシステムの構成を説明するための図である。
- 【図 14】自動ログインサイト情報などを自動更新する場合のブラウザの動作を説明するためのフローチャートである。
- 【図 15】第 3 の実施の形態に係る自動ログインシステムのシステム構成の一例を示した図である。
- 【図 16】第 4 の実施の形態に係る自動ログインシステムのシステム構成の一例を示した図である。
- 【図 17】従来例を説明するための図である。

【符号の説明】

1	自動ログインシステム	3	クライアント端末
5	サーバ	6	インターネット
7	非接触 IC カード	9	第 1 の鍵情報
10	ブラウザ	11	ブラウザ機能部
12	自動ログイン部	15	自動ログイン情報
16	自動ログインサイト情報	17	自動ログイン個人情報
21	IC カード R W	22	パスワード入力部
23	ブラウザ操作部	31	暗号・復号部
32	自動追加部	33	ログインリクエスト生成部
34	ログインリクエスト送信部	35	ブラウザ監視部
41	C P U	42	R O M
43	R A M	45	表示手段
46	入力手段	47	出力手段
48	通信制御手段	52	記憶媒体駆動装置
55	記憶装置	56	ブラウザプログラム
57	自動ログインサイト情報データベース		
58	自動ログイン個人情報データベース		



【図 1】



【図 2】

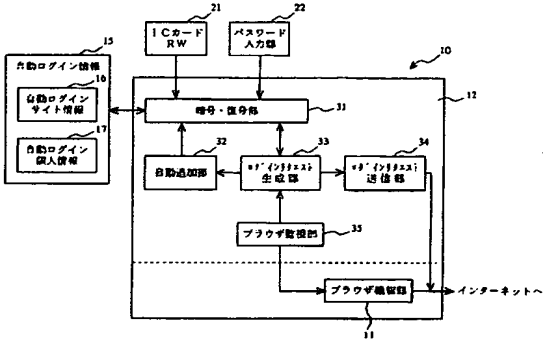
(a)  
自動ログインサイト情報 (第1の個人情報で符号化)

サービス名称	ログインページ情報	ログインリクエスト情報
サービス A	http://serverA.com/login.html	https://serverA.com/login.cgi?Lid=1Pec+52
サービス B	http://serverB.com/login.html	https://serverB.com/login.cgi?Lid=1Pec+52
...	...	...

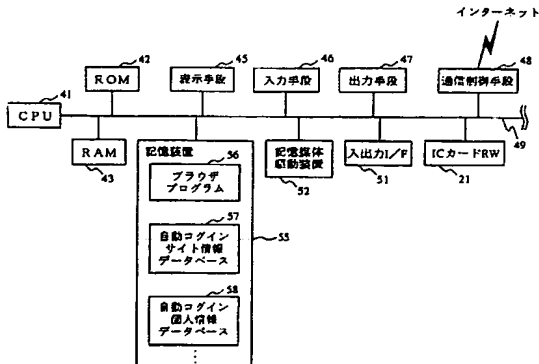
(b)  
自動ログイン個人情報 (第1の個人情報+第2の個人情報で符号化)

サービス名称	%1 (ログインID)	%2 (パスワード)	%3...
サービス A	userA	123	...
サービス B	userB	25427ab	...
...	...	...	...

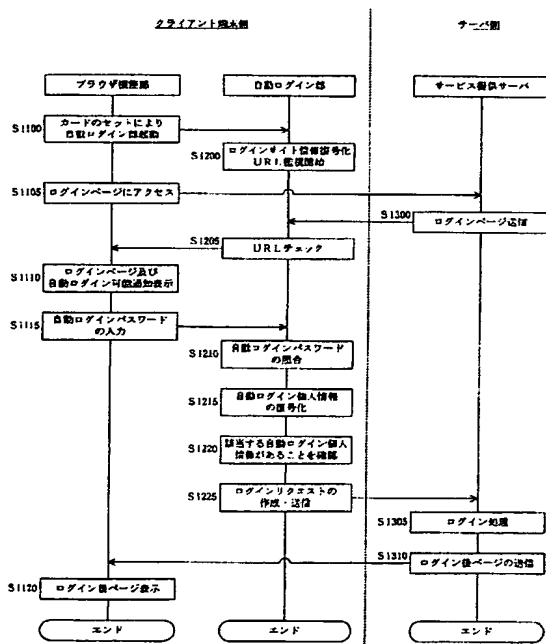
【図 3】



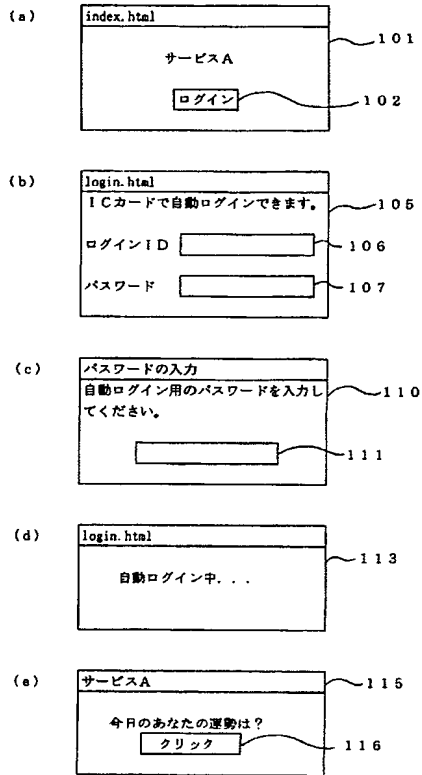
【図 4】



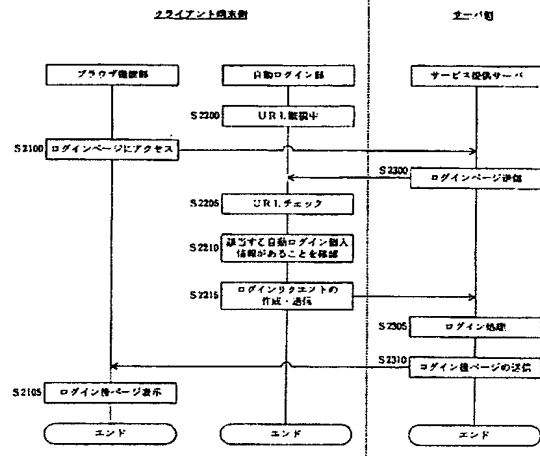
【図 5】



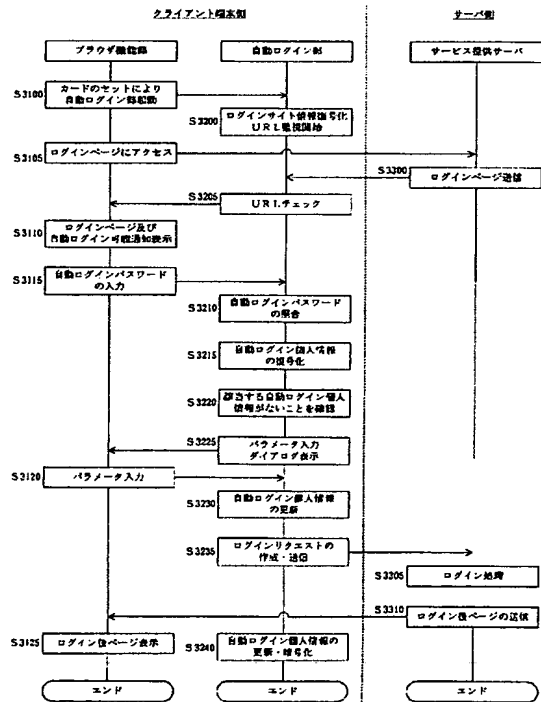
【図 6】



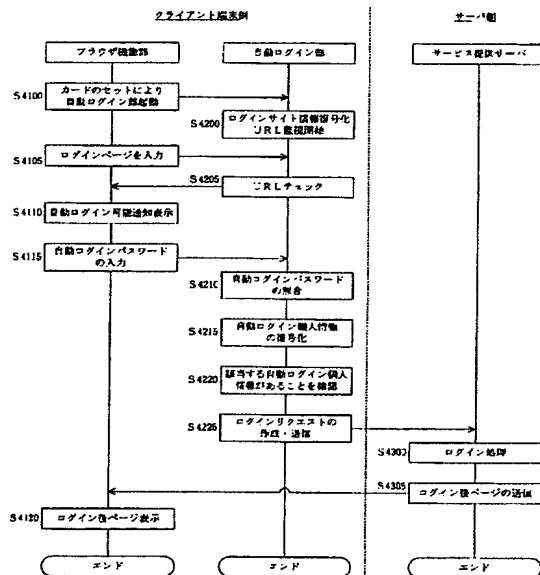
【図 7】



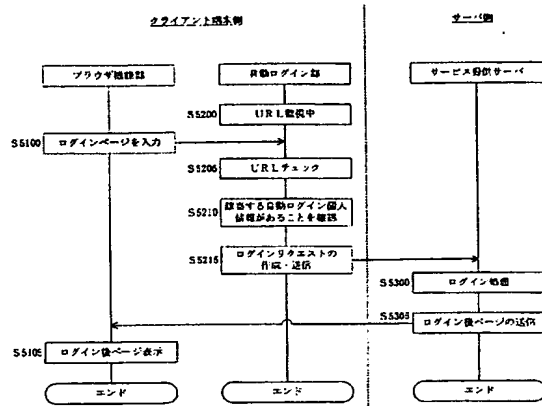
【図 8】



【図 9】



【図 10】



【図 11】

自動ログイン情報 (第1の識別情報+第2の識別情報で復号化)

160

サービス名称	ログインページ情報	第1の識別情報	%1 (第1 ID)	%2 (パスワード)	%3...
サービス A	http://serverA...	https://serverA...	userA	123	...
サービス B	http://serverB...	https://serverB...	userB	25487ab	...
...	...	...	...	...	...

【図 12】

(a)  
自動ログイン情報 (第1の識別情報で復号化)

160

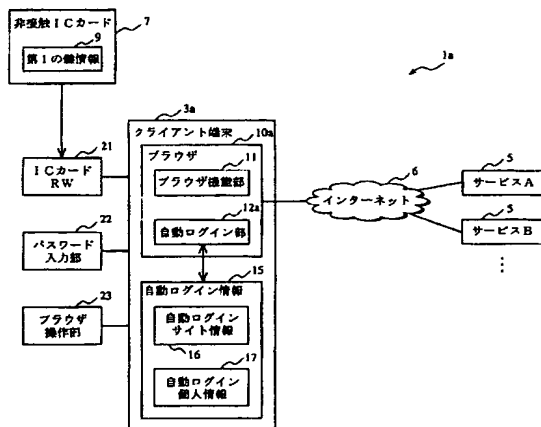
サービス名称	ログインページ情報	第1の識別情報	%1 (第1 ID)	%2 (パスワード)	%3...
サービス A	http://serverA...	https://serverA...	userA	123	...
サービス B	http://serverB...	https://serverB...	userB	25487ab	...
サービス C	http://serverC...	https://serverC...			
サービス D	http://serverD...	https://serverD...			
サービス E	http://serverE...	https://serverE...	userE	ab123cd	
...	...	...	...	...	...

(b)  
自動ログイン個人情報 (第1の識別情報+第2の識別情報で復号化)

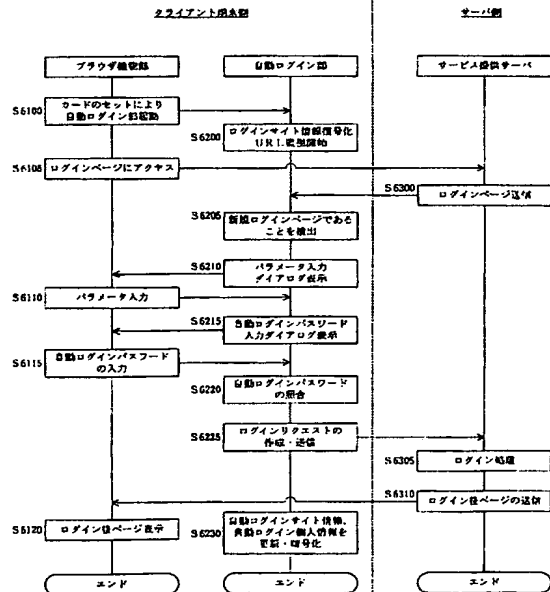
161

サービス名称	%1 (ログイン ID)	%2 (パスワード)	%3...
サービス A	userA	123	...
サービス B	userB	25487ab	...
サービス C	userC	efg456	...
サービス D	userD	hhtchseckels56e	...
サービス E	userE	ab123cd	...
...	...	...	...

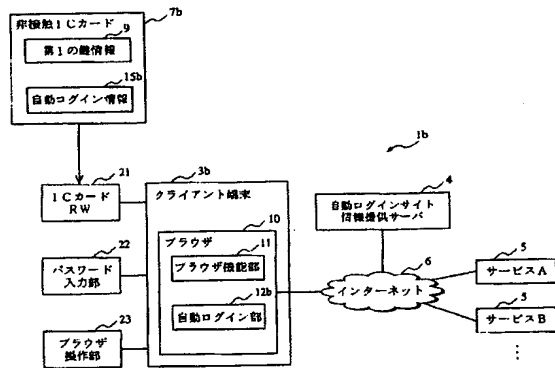
【図 13】



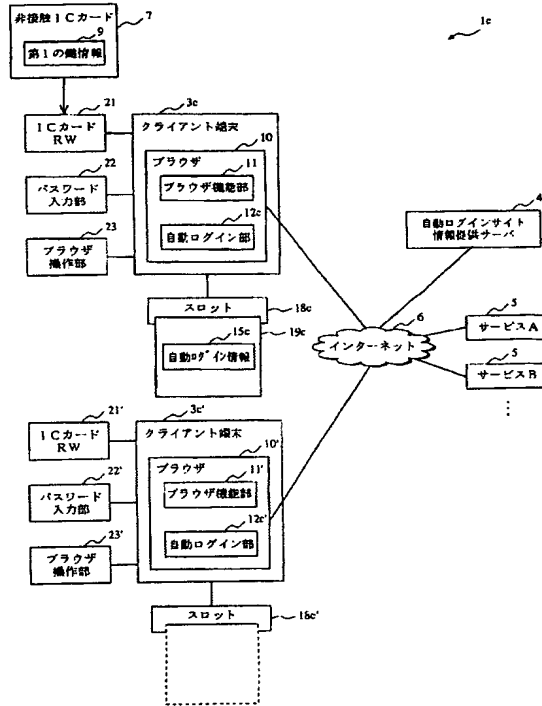
【図 14】



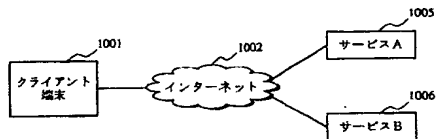
【図 15】



【図 16】



【図 17】



---

フロントページの続き

(51)Int. Cl.<sup>7</sup>

F I

テーマコード (参考)

H 0 4 L 9/00 6 7 3 E

H 0 4 L 9/00 6 7 5 ㄩ

(72)発明者 中山 浩

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 長島 敦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B085 AE01 AE08 AE13

5J104 AA07 EA03 NA05 NA38